NetFlow Configuration Guide, Cisco IOS Release 12.2SX

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Cisco IOS NetFlow Overview 1

Finding Feature Information 1

Information About Cisco IOS NetFlow 1

The NetFlow Application 2

NetFlow Benefits Monitoring Analysis and Planning Security and Accounting and Billing 2

NetFlow Cisco IOS Packaging Information 3

NetFlow Flows 3

NetFlow Main Cache Operation 4

NetFlow Data Capture 4

NetFlow Export Formats 4

NetFlow Operation Processing Order of NetFlow Features 5

NetFlow Preprocessing Features Filtering and Sampling 5

NetFlow Advanced Features and Services BGP Next Hop Multicast MPLS NetFlow Layer 2 6

NetFlow Postprocessing Features Aggregation Schemes and Export to Multiple Destinations 7

NetFlow MIBs 7

How to Configure Cisco IOS NetFlow 7

Configuration Examples for Cisco IOS NetFlow 8

Where to Go Next 8

Additional References 8

Glossary 10

Getting Started with Configuring Cisco IOS NetFlow and NetFlow Data Export 13

Finding Feature Information 13

Prerequisites for Configuring NetFlow and NetFlow Data Export 14

Restrictions for Configuring NetFlow and NetFlow Data Export 14

NetFlow Data Capture 14

NetFlow Data Export 15

Information About Configuring NetFlow and NetFlow Data Export 15

NetFlow Data Capture 15

NetFlow Flows Key Fields 16

NetFlow Data Export Using the Version 9 Export Format 16
How to Configure NetFlow and NetFlow Data Export 16
Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format 16
Verifying That NetFlow Is Operational and View NetFlow Statistics 18
Verifying That NetFlow Data Export Is Operational 21
Configuration Examples for Configuring NetFlow and NetFlow Data Export 21
Example Configuring Egress NetFlow Accounting 21
Example Configuring NetFlow Subinterface Support 22
Example Configuring NetFlow Multiple Export Destinations 22
Example Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format 22
Example Configuring NetFlow for Analyzing PPPoE Session Traffic 23
Additional References 23
Feature Information for Configuring NetFlow and NetFlow Data Export 25
Glossary 27
Configuring NetFlow and NetFlow Data Export 29
Finding Feature Information 29
Prerequisites for Configuring NetFlow and NetFlow Data Export 29
Restrictions for Configuring NetFlow and NetFlow Data Export 30
NetFlow Data Capture 30
NetFlow Data Export 31
Information About Configuring NetFlow and NetFlow Data Export 31
NetFlow Data Capture 32
NetFlow Flows Key Fields 32
NetFlow Cache Management and Data Export 32
NetFlow Export Format Versions 9 8 5 and 1 33
Overview 34
Details 34
NetFlow Export Version Formats 34
NetFlow Export Packet Header Format 35
NetFlow Flow Record and Export Format Content Information 36
NetFlow Data Export Format Selection 40
NetFlow Version 9 Data Export Format 41
NetFlow Version 8 Data Export Format 43
NetFlow Version 5 Data Export Format 44

NetFlow Version 1 Data Export Format 46
Egress NetFlow Accounting Benefits NetFlow Accounting Simplified 46
NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection 48
NetFlow Multiple Export Destinations Benefits 48
NetFlow on a Distributed VIP Interface 48
How to Configure NetFlow and NetFlow Data Export 48
Configuring NetFlow 48
Verifying that NetFlow Is Operational and Displaying NetFlow Statistics 50
Configuring NetFlow Data Export Using the Version 9 Export Format 52
Verifying that NetFlow Data Export Is Operational 55
Clearing NetFlow Statistics on the Router 56
Customizing the NetFlow Main Cache Parameters 57
NetFlow Cache Entry Management on a Routing Device 57
NetFlow Cache Size 58
Configuration Examples for Configuring NetFlow and NetFlow Data Export 61
Example Configuring Egress NetFlow Accounting 61
Example Configuring NetFlow Subinterface Support 61
NetFlow Subinterface Support for Ingress (Received) Traffic on a Subinterface 61
NetFlow SubInterface Support for Egress (Transmitted) Traffic on a Subinterface 61
Example Configuring NetFlow Multiple Export Destinations 62
Example Configuring NetFlow Version 5 Data Export 62
Example Configuring NetFlow Version 1 Data Export 63
Additional References 63
Feature Information for Configuring NetFlow and NetFlow Data Export 64
Glossary 66
Configuring NetFlow Aggregation Caches 69
Finding Feature Information 69
Prerequisites for Configuring NetFlow Aggregation Caches 69
Restrictions for Configuring NetFlow Aggregation Caches 70
NetFlow Data Export 70
Information About Configuring NetFlow Aggregation Caches 71
NetFlow Aggregation Caches 71
NetFlow Cache Aggregation Benefits 71
NetFlow Cache Aggregation Schemes 71
NetFlow Aggregation Scheme Fields 73

NetFlow AS Aggregation Scheme 75
NetFlow AS-ToS Aggregation Scheme 76
NetFlow Destination Prefix Aggregation Scheme 78
NetFlow Destination Prefix-ToS Aggregation Scheme 79
NetFlow Prefix Aggregation Scheme 81
NetFlow Prefix-Port Aggregation Scheme 82
NetFlow Prefix-ToS Aggregation Scheme 84
NetFlow Protocol Port Aggregation Scheme 86
NetFlow Protocol-Port-ToS Aggregation Scheme 87
NetFlow Source Prefix Aggregation Scheme 89
NetFlow Source Prefix-ToS Aggregation Scheme 90
NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview 92
How to Configure NetFlow Aggregation Caches 92
Configuring NetFlow Aggregation Caches 92
Verifying the Aggregation Cache Configuration 96
Configuration Examples for Configuring NetFlow Aggregation Caches 98
Configuring an AS Aggregation Cache Example 98
Configuring a Destination Prefix Aggregation Cache Example 99
Configuring a Prefix Aggregation Cache Example 99
Configuring a Protocol Port Aggregation Cache Example 99
Configuring a Source Prefix Aggregation Cache Example 100
Configuring an AS-ToS Aggregation Cache Example 100
Configuring a Prefix-ToS Aggregation Cache Example 100
Configuring the Minimum Mask of a Prefix Aggregation Scheme Example 101
Configuring the Minimum Mask of a Destination Prefix Aggregation Scheme Example 101
Configuring the Minimum Mask of a Source Prefix Aggregation Scheme Example 101
Configuring NetFlow Version 9 Data Export for Aggregation Caches Example 102
Configuring NetFlow Version 8 Data Export for Aggregation Caches Example 102
Additional References 102
Feature Information for Configuring NetFlow Aggregation Caches 104
Glossary 105
Configuring NetFlow BGP Next Hop Support for Accounting and Analysis 107
Finding Feature Information 107
Prerequisites for NetFlow BGP Next Hop Support 107
Restrictions for NetFlow BGP Next Hop Support 108

Information About NetFlow BGP Next Hop Support 108
NetFlow BGP Next Hop Support Benefits 108
NetFlow BGP Next Hop Support and NetFlow Aggregation 109
How to Configure NetFlow BGP Next Hop Support 109
Configuring NetFlow BGP Next Hop Accounting 109
Troubleshooting Tips 111
Verifying the Configuration 111
Configuration Examples for NetFlow BGP Next Hop Support 113
Example Configuring NetFlow BGP Next Hop Accounting 113
Additional References 113
Feature Information for NetFlow BGP Next Hop Support 114
Glossary 115
Configuring NetFlow BGP Next Hop Support for Accounting and Analysis 117
Finding Feature Information 117
Prerequisites for NetFlow BGP Next Hop Support 117
Restrictions for NetFlow BGP Next Hop Support 118
Information About NetFlow BGP Next Hop Support 118
NetFlow BGP Next Hop Support Benefits 118
NetFlow BGP Next Hop Support and NetFlow Aggregation 119
How to Configure NetFlow BGP Next Hop Support 119
Configuring NetFlow BGP Next Hop Accounting 119
Troubleshooting Tips 121
Verifying the Configuration 121
Configuration Examples for NetFlow BGP Next Hop Support 123
Example Configuring NetFlow BGP Next Hop Accounting 123
Additional References 123
Feature Information for NetFlow BGP Next Hop Support 124
Glossary 125
Configuring NetFlow Multicast Accounting 127
Finding Feature Information 127
Prerequisites for Configuring NetFlow Multicast Accounting 127
Restrictions for Configuring NetFlow Multicast Accounting 128
Information About Configuring NetFlow Multicast Accounting 128
NetFlow Multicast Benefits 128
Multicast Ingress and Multicast Egress Accounting 128

NetFlow Multicast Flow Records 129
How to Configure NetFlow Multicast Accounting 129
Configuring NetFlow Multicast Accounting in Releases 12.4(12) 129
Troubleshooting Tips 131
Configuring NetFlow Multicast Accounting in Cisco IOS Releases Prior to 12.4(12) 131
Configuring NetFlow Multicast Egress Accounting 131
Troubleshooting Tips 132
Configuring NetFlow Multicast Ingress Accounting 132
Troubleshooting Tips 134
Verifying the NetFlow Multicast Accounting Configuration 134
Configuration Examples for NetFlow Multicast Accounting 135
Configuring NetFlow Multicast Accounting in Original Releases 135
Configuring NetFlow MC Accounting in Releases Prior to 12.2(33)SRB 136
Configuring NetFlow Multicast Egress Accounting Example 136
Configuring NetFlow Multicast Ingress Accounting Example 136
Additional References 136
Feature Information for Configuring NetFlow Multicast Accounting 138
Glossary 139
Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands 141
Finding Feature Information 141
Prerequisites for Configuring NetFlow Top Talkers 141
Restrictions for Configuring NetFlow Top Talkers 142
Information About Configuring NetFlow Top Talkers 142
Overview of the NetFlow MIB and Top Talkers Feature 142
Benefits of the NetFlow MIB and Top Talkers Feature 143
Cisco IOS Release 12.2(33)SXH on Cisco 6500 Series Switches 143
How to Configure NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP
Commands 143
Configuring SNMP Support on the Networking Device 144
Configuring Parameters for the NetFlow Main Cache 145
Configuring Parameters for the NetFlow Main Cache 147
Identifying the Interface Number to Use for Enabling NetFlow with SNMP 147
Configuring NetFlow on a Cisco 6500 Series Switch 148
Configuring NetFlow on a Cisco 6500 Series Switch 150
Configuring NetFlow on Cisco Routers 151

Configuring NetFlow on Cisco Routers 153
Configuring NetFlow Top Talkers 153
Configuring NetFlow Top Talkers 155
Configuring NetFlow Top Talkers Match Criteria 156
NetFlow Top Talkers Match Criteria Specified by CLI Commands 157
NetFlow Top Talkers Match Criteria Specified by SNMP Commands 157
Configuring Source IP Address Top Talkers Match Criteria 159
Configuring Source IP Address Top Talkers Match Criteria 160
Verifying the NetFlow Top Talkers Configuration 161
Verifying the NetFlow Top Talkers Configuration 162
Configuration Examples for NetFlow Top Talkers 163
Configuring NetFlow Top Talkers Using SNMP Commands Example 163
Configuring NetFlow Top Talkers Match Criteria Using SNMP Commands Example 164
Additional References 164
Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands 166
Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces 169
Finding Feature Information 169
Prerequisites for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces 170
Restrictions for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces 170
Information About NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces 170
GRE Tunneling 170
GRE Tunnel Keepalive 171
Tunnel Interfaces 171
NetFlow Accounting on GRE IP Tunnel Interfaces 171
How to Configure NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces 175
Sample Network 176
Configuring a GRE IP Tunnel 176
Verifying the Status of the GRE IP Tunnel 180
Configuring NetFlow Accounting on a GRE IP Tunnel Interface 181
Configuring NetFlow Accounting on the Physical Interfaces 182
Verifying NetFlow Accounting 184
Configuring NetFlow Data Export Using the Version 9 Export Format 186
Verifying That NetFlow Data Export Is Operational 189

Configuration Examples for NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces 190

Configuring a GRE IP Tunnel Example 190

Configuring NetFlow Accounting on a GRE IP Tunnel Example 191

Additional References 192

Feature Information for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces 193

Cisco IOS NetFlow Overview

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology. This module provides an overview of the NetFlow application and advanced NetFlow features and services.

- Finding Feature Information, page 1
- Information About Cisco IOS NetFlow, page 1
- How to Configure Cisco IOS NetFlow, page 7
- Configuration Examples for Cisco IOS NetFlow, page 8
- Where to Go Next, page 8
- Additional References, page 8
- Glossary, page 10

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco IOS NetFlow

- The NetFlow Application, page 2
- NetFlow Benefits Monitoring Analysis and Planning Security and Accounting and Billing, page 2
- NetFlow Cisco IOS Packaging Information, page 3
- NetFlow Flows, page 3
- NetFlow Main Cache Operation, page 4
- NetFlow Data Capture, page 4
- NetFlow Export Formats, page 4
- NetFlow Operation Processing Order of NetFlow Features, page 5
- NetFlow Preprocessing Features Filtering and Sampling, page 5
- NetFlow Advanced Features and Services BGP Next Hop Multicast MPLS NetFlow Layer 2, page 6

- NetFlow Postprocessing Features Aggregation Schemes and Export to Multiple Destinations, page 7
- NetFlow MIBs, page 7

The NetFlow Application

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow identifies packet flows for both ingress and egress IP packets. It does not involve any connection-setup protocol, either between routers or to any other networking device or end station. NetFlow does not require any change externally--either to the packets themselves or to any networking device. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow capture and export are performed independently on each internetworking device; NetFlow need not be operational on each router in the network.

NetFlow is supported on IP and IP encapsulated traffic over most interface types and encapsulations. However, NetFlow does not support ATM LAN emulation (LANE) and does not support an Inter-Switch Link (ISL)/virtual LAN (VLAN), ATM, or Frame Relay interfaces when more than one input access control list (ACL) is used on the interface. Cisco 12000 IP Service Engine ATM line cards do not have this restriction when more than one input ACL is used on the interface.

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution data, IP flow switching cache information, and flow information. See the NetFlow Flows, page 3.

NetFlow Benefits Monitoring Analysis and Planning Security and Accounting and Billing

NetFlow captures a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service (ToS) information that can be used for a wide variety of purposes such as network application and user monitoring, network analysis and planning, security analysis, accounting and billing, traffic engineering, and NetFlow data warehousing and data mining.

Network Application and User Monitoring

NetFlow data enables you to view detailed, time- and application-based usage of a network. This information allows you to plan and allocate network and application resources, and provides for extensive near real-time network monitoring capabilities. It can be used to display traffic patterns and application-based views. NetFlow provides proactive problem detection and efficient troubleshooting, and it facilitates rapid problem resolution. You can use NetFlow information to efficiently allocate network resources and to detect and resolve potential security and policy violations.

Network Planning

NetFlow can capture data over a long period of time, which enables you to track and anticipate network growth and plan upgrades. NetFlow service data can be used to optimize network planning, which includes peering, backbone upgrade planning, and routing policy planning. It also enables you to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and quality of service (QoS) usage, and enables the analysis of new network applications. NetFlow offers valuable information that you can use to reduce the cost of operating the network.

Denial of Service and Security Analysis

You can use NetFlow data to identify and classify denial of service (DoS) attacks, viruses, and worms in real-time. Changes in network behavior indicate anomalies that are clearly reflected in NetFlow data. The data is also a valuable forensic tool that you can use to understand and replay the history of security incidents.

>Accounting and Billing

NetFlow data provides fine-grained metering for highly flexible and detailed resource utilization accounting. For example, flow data includes details such as IP addresses, packet and byte counts, timestamps, type-of-service, and application ports. Service providers might utilize the information for billing based on time-of-day, bandwidth usage, application usage, or quality of service. Enterprise customers might utilize the information for departmental chargeback or cost allocation for resource utilization.

Traffic Engineering

NetFlow provides autonomous system (AS) traffic engineering details. You can use NetFlow-captured traffic data to understand source-to-destination traffic trends. This data can be used for load-balancing traffic across alternate paths or for forwarding traffic to a preferred route. NetFlow can measure the amount of traffic crossing peering or transit points to help you determine if a peering arrangement with other service providers is fair and equitable.

>NetFlow Data Storage and Data Mining

NetFlow data (or derived information) can be stored for later retrieval and analysis in support of marketing and customer service programs. For example, the data can be used to find out which applications and services are being used by internal and external users and to target those users for improved service and advertising. In addition, NetFlow data gives market researchers access to the who, what, where, and how long information relevant to enterprises and service providers.

NetFlow Cisco IOS Packaging Information

Cisco 7200/7500/7400/MGX/AS5800

Although NetFlow functionality is included in all software images for these platforms, you must purchase a separate NetFlow feature license. NetFlow licenses are sold on a per-node basis.

>Other Routers

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

NetFlow Flows

A NetFlow network flow is defined as a unidirectional stream of packets between a given source and destination. The source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is defined by the combination of the following seven key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might also contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format), depending on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Main Cache Operation

The key components of NetFlow are the NetFlow cache that stores IP flow information, and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. NetFlow maintains a flow record within the cache for each active flow. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine.

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers data for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers data for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers data for all egress MPLS-to-IP packets.

NetFlow Export Formats

NetFlow exports data in UDP datagrams in one of five formats: Version 9, Version 8, Version 7, Version 5, or Version 1. Version 9 export format, the latest version, is the most flexible and extensive format. Version 1 was the initial NetFlow export format; Version 7 is supported only on certain platforms, and Version 8 only supports export from aggregation cache. (Versions 2 through 4 and Version 6 were either not released or are not supported.)

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. The distinguishing feature of the NetFlow Version 9 format is that it is template based. Templates provide a means of extending the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Internet Protocol Information Export (IPFIX) was based on the Version 9 export format.

- Version 8--A format added to support data export from aggregation caches. Version 8 allows export datagrams to contain a subset of the usual Version 5 export data, if that data is valid for a particular aggregation cache scheme.
- Version 7--A version supported on Catalyst 6000 series switches with a Multilayer Switch Feature Card (MSFC) on CatOS Release 5.5(7) and later.

On Catalyst 6000 series switches with an MSFC, you can export using either the Version 7 or Version 8 format.

Information about and instructions for configuring NetFlow on Catalyst 6000 series switches is available in the Catalyst 6500 Series Switches documentation.

- Version 5--A version that adds BGP autonomous system (AS) information and flow sequence numbers.
- Version 1, the initially released export format, is rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format for data export from the main cache.

For more information on a specific NetFlow data export format, see the "Configuring NetFlow and NetFlow Data Export" module.

NetFlow Operation Processing Order of NetFlow Features

The NetFlow application supports features that you can set up to further analyze network traffic data. NetFlow divides these features and services into the following three categories for processing:

- Preprocessing features that allow you to collect subsets of your network traffic data for analysis.
- Advanced features and services based on the flexible NetFlow Version 9 export format that allow you to collect data on types of traffic in addition to IP traffic.
- Postprocessing features that allow you to define fields that control how traffic data is exported.

You need to decide if you want to further analyze your network traffic. If you do want to do further analysis, you need to make choices in two areas:

- Do you want to customize or fine-tune the way that you collect NetFlow data? For example, you might want to configure packet sampling, or packet filtering, or an aggregation scheme.
- Do you want to collect and analyze data about the use of other Cisco IOS applications? For example, you might want to configure NetFlow support for BGP next hop, multicast, MPLS, or IPv6.

Before you configure or enable an additional NetFlow feature or service, you need to understand the prerequisites, restrictions, and key concepts that apply to each feature or service. Refer to the following sections for information about and links to the NetFlow features and services:

NetFlow Preprocessing Features Filtering and Sampling

The table below briefly describes preprocessing features and indicates where you can find concept and task information about each. You set up these features to select the subset of traffic of interest to you before NetFlow processing begins.

Table 1 NetFlow Preprocessing Features

Preprocessing Feature	Brief Description	Source for Concept and Task Information
Packet sampling	Sets up statistical sampling of network traffic for traffic engineering or capacity planning	See the "Using NetFlow Filtering or Sampling to Select the Network Traffic to Track" module.
Filtering	Sets up a specific subset of network traffic for class-based traffic analysis and monitoring on-network or off-network traffic	See the "Using NetFlow Filtering or Sampling to Select the Network Traffic to Track" module.

NetFlow Advanced Features and Services BGP Next Hop Multicast MPLS NetFlow Layer 2

The table below briefly describes advanced features and services supported by NetFlow and indicates where you can find concept and task information about each. Configure these features and services to collect and analyze NetFlow traffic statistics about them (features such as BGP Next Hop, multicast, and MPLS).

Table 2 NetFlow Advanced Features and Services

Feature or Service	Brief Description	Source for Concept and Task Information
BGP next hop support	Sets up the export of BGP next hop information for the purpose of measuring network traffic on a per BGP next hop basis	See the "Configuring NetFlow BGP Next Hop Support for Accounting and Analysis" module.
Multicast support	Sets up the capture of multicast-specific data that allows you to get a complete multicast traffic billing solution	See the "Configuring NetFlow Multicast Accounting" module.
MPLS support	Sets up the capture of MPLS traffic containing both IP and non-IP packets for use in MPLS network management, network planning, and enterprise accounting	See the "Configuring MPLS-aware NetFlow" module.
NetFlow Layer 2 and Security Monitoring Exports	Sets up the capture of Layer 2 and Layer 3 fields for use in security monitoring, network management, network planning, and enterprise accounting	See the "NetFlow Layer 2 and Security Monitoring Exports" module.

NetFlow Postprocessing Features Aggregation Schemes and Export to Multiple Destinations

The table below briefly describes postprocessing features and indicates where you can find concept and task information about each. You configure these features to set up the export of NetFlow data.

Table 3 NetFlow Postprocessing Features

Postprocessing Features	Brief Description	Source for Concept and Task Information
Aggregation schemes	Sets up extra aggregation caches with different combinations of fields that determine which traditional flows are grouped together and collected when a flow expires from the main cache	"Configuring NetFlow Aggregation Caches"
Export to multiple destinations	Sets up identical streams of NetFlow data to be sent to multiple hosts	"Configuring NetFlow and NetFlow Data Export"

NetFlow MIBs

The NetFlow MIB and the NetFlow MIB and Top Talkers features provide real time access to NetFlow cache information. These feature do not require a collector to obtain NetFlow data. This allows smaller enterprises to collect NetFlow data.

With the NetFlow MIB feature, you can access in real time the system information that is stored in the NetFlow cache by utilizing a MIB implementation based on the Simple Network Management Protocol (SNMP). This information is accessed by **get** and **set** commands entered on the network management system (NMS) workstation for which SNMP has been implemented. The NetFlow MIB feature provides MIB objects that allow you to monitor cache flow information, the current NetFlow configuration, and statistics. For details about the NetFlow MIB, see the "Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data" module.

The NetFlow MIB and Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. You can use this feature for security monitoring or accounting purposes for top talkers, and matching and identifying addresses for key users of the network. You configure the criteria by which flows from the NetFlow cache are sorted and placed in a special cache. The flows that are displayed by this feature are known as "top talkers." For details about the NetFlow MIB and Top Talkers, see the "Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands" module.

How to Configure Cisco IOS NetFlow

There are no tasks for the "Cisco IOS NetFlow Overview" module.

See the "Additional References" section for links to configuration information for NetFlow features and services.

Configuration Examples for Cisco IOS NetFlow

There are no configuration examples for the "Cisco IOS NetFlow Overview" module.

See the "Additional References" section for links to configuration information for NetFlow features and services.

Where to Go Next

To configure basic NetFlow, refer to the "Configuring NetFlow and NetFlow Data Export" module. See the "Additional References" section for links to configuration information about additional NetFlow features and services.

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	"Cisco IOS NetFlow Overview"
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	"Getting Started with Configuring NetFlow and NetFlow Data Export"
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	"Configuring NetFlow Aggregation Caches"
Tasks for configuring NetFlow BGP next hop support	"Configuring NetFlow BGP Next Hop Support for Accounting and Analysis"
Tasks for configuring NetFlow multicast support	"Configuring NetFlow Multicast Accounting"
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow

Related Topic	Document Title
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	"NetFlow Layer 2 and Security Monitoring Exports"
Tasks for configuring the SNMP NetFlow MIB	"Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data"
Tasks for configuring the NetFlow MIB and Top Talkers feature	"Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands"
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	"Cisco CNS NetFlow Collection Engine Documentation"

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
• RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
• RFC 3954	Cisco Systems NetFlow Services Export Version 9

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided into areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a certain destination.

flow --(NetFlow) A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

IPv6 --IP Version 6. Replacement for the current version of IP (Version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

ISL --Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

MPLS --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along normally routed paths (sometimes called MPLS hop-by-hop forwarding).

multicast --When single packets are copied by the network and sent to a specific subset of network addresses, they are said to be multicast. These addresses are specified in the Destination Address field.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router or switch that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow V9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

QoS --quality of service. A measure of performance for a transmission system that reflects the system's transmission quality and service availability.

traffic engineering --Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

VLAN --virtual LAN. Group of devices on one or more LANs that are configured (by management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

Getting Started with Configuring Cisco IOS NetFlow and NetFlow Data Export

This module contains the minimum amount of information about and instructions necessary for configuring NetFlow to capture and export network traffic data. This module is intended to help you get started using NetFlow and NetFlow Data Export as quickly as possible. If you want more detailed information about this feature and instructions for configuring NetFlow and NetFlow Data Export, please refer to Configuring NetFlow and NetFlow Data Export.

NetFlow capture and export are performed independently on each internetworking device on which NetFlow is enabled. NetFlow need not be operational on each router in the network.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. NetFlow is emerging as a primary network accounting and security technology.

- Finding Feature Information, page 13
- Prerequisites for Configuring NetFlow and NetFlow Data Export, page 14
- Restrictions for Configuring NetFlow and NetFlow Data Export, page 14
- Information About Configuring NetFlow and NetFlow Data Export, page 15
- How to Configure NetFlow and NetFlow Data Export, page 16
- Configuration Examples for Configuring NetFlow and NetFlow Data Export, page 21
- Additional References, page 23
- Feature Information for Configuring NetFlow and NetFlow Data Export, page 25
- Glossary, page 27

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring NetFlow and NetFlow Data Export

Before you enable NetFlow:

- Configure the router for IP routing.
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching.
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources.

Restrictions for Configuring NetFlow and NetFlow Data Export

- NetFlow Data Capture, page 14
- NetFlow Data Export, page 15

NetFlow Data Capture

NetFlow consumes additional memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a smaller number of entries. The default cache size depends on the platform. For example, the default cache size for the Cisco 7500 router is 65536 (64K) entries.

Memory Impact

During times of heavy traffic, the additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T, the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later, the **ip flow ingress** command is used to enable NetFlow on an interface.

Egress NetFlow Accounting in Cisco IOS 12.3T Releases, 12.3(11)T, or Later

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. MPLS statistics are not captured. The MPLS Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrived at the router as MPLS packets and underwent label disposition.

Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

Locally generated traffic (traffic that is generated by the router on which the Egress NetFlow Accounting feature is configured) is not counted as flow traffic for the Egress NetFlow Accounting feature.

Note In Cisco IOS 12.2S releases, egress NetFlow captures either IPv4 packets or MPLS packets as they leave the router.

The Egress NetFlow Accounting feature counts CEF-switched packets only. Process-switched transit packets are not counted.

NetFlow Data Export

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets) versus Version 5. The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

Information About Configuring NetFlow and NetFlow Data Export

- NetFlow Data Capture, page 15
- NetFlow Flows Key Fields, page 16
- NetFlow Data Export Using the Version 9 Export Format, page 16

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers statistics for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers statistics for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers statistics for all egress MPLS-to-IP packets.

NetFlow Flows Key Fields

A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and by transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format) that depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Data Export Using the Version 9 Export Format

NetFlow Data Export format Version 9 is a flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. The Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.

How to Configure NetFlow and NetFlow Data Export

- Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format, page 16
- Verifying That NetFlow Is Operational and View NetFlow Statistics, page 18
- Verifying That NetFlow Data Export Is Operational, page 21

Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format

Perform this task to configure NetFlow and NetFlow Data Export using the Version 9 export format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*
4. Repeat Step 3 once to configure a second NetFlow export destination.
5. **ip flow-export version 9**
6. **interface** *interface-type interface-number*
7. **ip flow** {**ingress** | **egress**}
8. **exit**
9. Repeat Steps 6 through 8 to enable NetFlow on other interfaces
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	(Optional) IP address or hostname of the workstation to which you want to send the NetFlow information and the number of the UDP port on which the workstation is listening for this input. **Note** The workstation is running an application such as NetFlow Collection Engine (NFC) that is used to analyze the exported data.
Step 4	Repeat Step 3 once to configure a second NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.

	Command or Action	Purpose
Step 5	**ip flow-export version 9** **Example:** `Router(config)# ip flow-export version 9`	(Optional) Enables the export of information in NetFlow cache entries. • The **version 9**keyword specifies that the export packet uses the Version 9 format. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card CEF tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 6	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 7	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface. • **egress** --Captures traffic that is being transmitted by the interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 9	Repeat Steps 6 through 8 to enable NetFlow on other interfaces	(Optional) --
Step 10	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Verifying That NetFlow Is Operational and View NetFlow Statistics

To verify that NetFlow is working properly, perform this optional task.

SUMMARY STEPS

1. **show ip flow interface**
2. **show ip cache flow**
3. **show ip cache verbose flow**

DETAILED STEPS

Step 1 **show ip flow interface**

Use this command to display the NetFlow configuration for an interface. The following is sample output from this command:

Example:

```
Router# show ip flow interface
Ethernet0/0
  ip flow ingress
```

Step 2 **show ip cache flow**

Use this command to verify that NetFlow is operational and to display a summary of the NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.8    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.1    1799.6       0.9
ICMP               135      0.0      1133   427      3.1    1799.6       0.8
Total:             945      0.0      1166    91     22.4    1799.6       0.8
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.67.6    Et1/0.1       172.16.10.200   01 0000 0C01    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0043 0043    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0045 0045    51
Et0/0         10.234.53.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 0044 0044    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 00A2 00A2    51
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0014 0014    50
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0015 0015    52
.
.
.
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0087 0087    50
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0050 0050    51
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0089 0089    49
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0050 0050    50
```

```
Et0/0         10.251.10.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.162.37.71    Null          172.16.11.3     06 027C 027C    49
```

Step 3 **show ip cache verbose flow**

Use this command to verify that NetFlow is operational and to display a detailed summary of the NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (1130681 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2992518 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.6    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.0    1799.6       0.9
ICMP               135      0.0      1133   427      3.0    1799.6       0.8
Total:             945      0.0      1166    91     21.9    1799.6       0.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0          192.168.67.6    Et1/0.1        172.16.10.200   01 00  10     799
0000 /0  0                     0C01 /0  0     0.0.0.0                28  1258.1
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0043 /0  0                     0043 /0  0     0.0.0.0                28  1258.0
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0045 /0  0                     0045 /0  0     0.0.0.0                28  1258.0
Et0/0          10.234.53.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0                28  1258.1
Et0/0          10.10.19.1      Null           172.16.11.6     11 00  10     799
0044 /0  0                     0044 /0  0     0.0.0.0                28  1258.1
.
.
.
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0087 /0  0                     0087 /0  0     0.0.0.0                40  1258.1
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     798
0089 /0  0                     0089 /0  0     0.0.0.0                40  1256.5
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
Et0/0          10.251.10.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0              1500  1258.1
Et0/0          10.162.37.71    Null           172.16.11.3     06 00  00     798
027C /0  0                     027C /0  0     0.0.0.0                40  1256.4
```

Verifying That NetFlow Data Export Is Operational

To verify that NetFlow data export is operational and to view the statistics for NetFlow data export perform the step in this optional task.

SUMMARY STEPS

1. **show ip flow export**

DETAILED STEPS

---

show ip flow export
Use this command to display the statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

Example:

```
Router# show ip flow export
Flow export v9 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source interface Ethernet0/0
  Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Configuration Examples for Configuring NetFlow and NetFlow Data Export

- Example Configuring Egress NetFlow Accounting, page 21
- Example Configuring NetFlow Subinterface Support, page 22
- Example Configuring NetFlow Multiple Export Destinations, page 22
- Example Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format, page 22
- Example Configuring NetFlow for Analyzing PPPoE Session Traffic, page 23

Example Configuring Egress NetFlow Accounting

The following example shows how to configure Egress NetFlow Accounting:

```
configure terminal
!
interface ethernet 0/0
```

```
 ip flow egress
!
```

Example Configuring NetFlow Subinterface Support

NetFlow Subinterface Support For Ingress (Received) Traffic On a Subinterface

```
configure terminal
!
interface ethernet 0/0.1
 ip flow ingress
!
```

NetFlow SubInterface Support For Egress (Transmitted) Traffic On a Subinterface

```
configure terminal
!
interface ethernet 1/0.1
 ip flow egress
!
```

Note NetFlow performs additional checks for the status of each subinterface that requires more CPU processing time and bandwidth. If you have several subinterfaces configured and you want to configure NetFlow data capture on all of them, we recommend that you configure NetFlow on the main interface instead of on the individual subinterfaces.

Example Configuring NetFlow Multiple Export Destinations

The following example shows how to configure NetFlow multiple export destinations:

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export destination 172.16.10.2 9991
!
```

Note You can configure a maximum of two export destinations for the main cache and for each aggregation cache.

Example Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format

The following example shows how to configure NetFlow and NetFlow data export using the Version 9 export format:

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export version 9
!
```

Example Configuring NetFlow for Analyzing PPPoE Session Traffic

If you want to obtain accurate NetFlow traffic statistics for PPPoE sessions, you must configure NetFlow on the virtual-template interface, not on the physical interface that is configured with VLAN encapsulation. For example, if you configure NetFlow on the physical interface that is configured for VLAN encapsulation as shown in the following configuration, the NetFlow traffic statistics will not be an accurate representation of the traffic on the PPPoE sessions.

```
!
interface GigabitEthernet2/0/0.10
 encapsulation dot1Q 10
 ip flow egress
 pppoe enable
```

The following example shows how to configure egress NetFlow on a virtual template interface so that you can accurately analyze the packet size distribution statistics of the traffic that the router is sending to the end user over the PPoE session:

```
interface Virtual-Template 1
 ip unnumbered ethernet 0
 encapsulation ppp
 ip flow egress
```

The following display output from the **show ip cache flow** command shows that this PPPoE session traffic is comprised primarily of 1536-byte packets.

```
Router# show ip cache flow
IP packet size distribution (11014160 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .000 .000 .000 .999 .000 .000 .000 .000 .000 .000
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track

Related Topic	Document Title
Tasks for configuring random sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation
Configuration commands for NetFlow	*Cisco IOS NetFlow Command Reference*

Standards

Standards	Title
No new or modified standards are supported , and support for existing standards has not been modified.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified .	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring NetFlow and NetFlow Data Export

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4 Feature Information for Configuring NetFlow and NetFlow Data Export

Feature Name	Releases	Feature Configuration Information
Egress NetFlow Accounting	12.3(11)T 15.0(1)S	The Egress NetFlow Accounting feature allows NetFlow statistics to be gathered on egress traffic that is exiting the router. Previous versions of NetFlow allow statistics to be gathered only on ingress traffic that is entering the router. The following commands were introduced by this feature: **ip flow egress** and **ip flow-egress input-interface**. The following commands were modified by this feature: **flow-sampler**, **match**, **show ip cache flow**, **show ip cache verbose flow**, and **show ip flow interface**.
NetFlow Multiple Export Destinations	12.0(19)S 12.2(2)T 12.2(14)S 15.0(1)S	The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. The following commands were modified by this feature: **ip flow-aggregation cache**, **ip flow-export destination**, and **show ip flow export**.
NetFlow Subinterface Support	12.0(22)S 12.2(14)S 12.2(15)T	The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. The following command was introduced by this feature: **ip flow ingress**. The following command was modified by this feature: **show ip interface**.

Feature Name	Releases	Feature Configuration Information
NetFlow v9 Export Format	12.0(24)S 12.2(18)S 12.2(27)SBC 12.2(18)SXF 12.3(1) 15.0(1)S	The NetFlow v9 Export Format is flexible and extensible, which provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, NAT, and BGP next hop. The following commands were modified by this feature: **debug ip flow export**, **export**, **ip flow-export**, and **show ip flow export**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

CEF --Cisco Express Forwarding. Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used by a router to reach a certain destination.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --Type of packet built by a device (for example, a router) with NetFlow services enabled that is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information on IP flows).

fast switching --Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

MPLS --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along a normally routed path (sometimes called MPLS hop-by-hop forwarding).

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine.

This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

RP --Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a Supervisory Processor.

Configuring NetFlow and NetFlow Data Export

This module contains information about and instructions for configuring NetFlow to capture and export network traffic data. NetFlow capture and export are performed independently on each internetworking device on which NetFlow is enabled. NetFlow need not be operational on each router in the network.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. NetFlow is a primary network accounting and security technology.

- Finding Feature Information, page 29
- Prerequisites for Configuring NetFlow and NetFlow Data Export, page 29
- Restrictions for Configuring NetFlow and NetFlow Data Export, page 30
- Information About Configuring NetFlow and NetFlow Data Export, page 31
- How to Configure NetFlow and NetFlow Data Export, page 48
- Configuration Examples for Configuring NetFlow and NetFlow Data Export, page 61
- Additional References, page 63
- Feature Information for Configuring NetFlow and NetFlow Data Export, page 64
- Glossary, page 66

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring NetFlow and NetFlow Data Export

Before you enable NetFlow, you must do the following:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding, distributed Cisco Express Forwarding, or fast switching

- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources

Restrictions for Configuring NetFlow and NetFlow Data Export

- NetFlow Data Capture, page 30
- NetFlow Data Export, page 31

NetFlow Data Capture

NetFlow consumes a significant amount of memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a lower number of entries. The default cache size depends on the platform. For example, the default cache size for the Cisco 7500 router is 65,536 (64K) entries.

Memory Impact

During times of heavy traffic, additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T, the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or a later release, use the **ip flow ingress** command to enable NetFlow on an interface.

Cisco IOS Releases 12.4(20)T or Earlier Releases

The **ip flow ingress** command behavior depends on the Cisco IOS release:

If your router is running a version earlier than Cisco IOS Release 12.4(20)T, and your router does not have a VPN Service Adapter (VSA)-enabled interface, enabling the **ip flow ingress**command will result in the ingress traffic being accounted for twice by the router.

If your router is running a version earlier than Cisco IOS Release 12.4(20)T, and your router has a VSA-enabled interface, enabling the **ip flow ingress** command will result in the encrypted ingress traffic being accounted for only once.

If your router is running a version of Cisco IOS Release12.4(20)T or later, enabling the **ip flow ingress** command will result in the encrypted ingress traffic being accounted for only once.

Egress NetFlow Accounting in Cisco IOS 12.3T Releases, 12.3(11)T, or Later Releases

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. Multiprotocol Label Switching (MPLS) statistics are not captured. The MPLS Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrive at the router as MPLS packets and undergo label disposition.

Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

Locally generated traffic (traffic that is generated by the router on which the Egress NetFlow Accounting feature is configured) is not counted as flow traffic for the Egress NetFlow Accounting feature.

Note In Cisco IOS 12.2S releases, egress NetFlow captures either IPv4 or MPLS packets as they leave the router.

NetFlow Data Export

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--The export bandwidth use increases for Version 9 (because of template flowsets) when compared to Version 5. The increase in bandwidth usage varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets; this has a bandwidth cost of about 4 percent. If required, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases the overall performance because generating and maintaining valid template flowsets requires additional processing.

Restrictions for NetFlow Version 8 Export Format

Version 8 export format is available only for aggregation caches; it cannot be expanded to support new features.

Restrictions for NetFlow Version 5 Export Format

Version 5 export format is suitable only for the main cache; it cannot be expanded to support new features.

Restrictions for NetFlow Version 1 Export Format

The Version 1 format was the initially released version. Do not use the Version 1 format unless you are using a legacy collection system that requires it. Use Version 9 or Version 5 export format.

Information About Configuring NetFlow and NetFlow Data Export

- NetFlow Data Capture, page 32
- NetFlow Flows Key Fields, page 32
- NetFlow Cache Management and Data Export, page 32
- NetFlow Export Format Versions 9 8 5 and 1, page 33
- Egress NetFlow Accounting Benefits NetFlow Accounting Simplified, page 46
- NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection, page 48
- NetFlow Multiple Export Destinations Benefits, page 48
- NetFlow on a Distributed VIP Interface, page 48

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers statistics for the following ingress IP packets:

- IP-to-IP packets
- IP-to-MPLS packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers statistics for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers statistics for all egress MPLS-to-IP packets.

NetFlow Flows Key Fields

A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field that is different from another packet, it is considered to belong to another flow. A flow might contain other accounting fields (such as the autonomous system number in the NetFlow export Version 5 flow format) that depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Cache Management and Data Export

The key components of NetFlow are the NetFlow cache or data source that stores IP flow information and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. A flow record is maintained within the NetFlow cache for each active flow. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device such as the NetFlow Collection Engine.

NetFlow is efficient, with the amount of export data being about 1.5 percent of the switched traffic in the router. NetFlow accounts for every packet (nonsampled mode) and provides a highly condensed and detailed view of all network traffic that enters the router or switch.

The key to NetFlow-enabled switching scalability and performance is highly intelligent flow cache management, especially for densely populated and busy edge routers handling large numbers of concurrent, short duration flows. The NetFlow cache management software contains a highly sophisticated set of algorithms for efficiently determining whether a packet is part of an existing flow or whether the packet requires a new flow cache entry. The algorithms are also capable of dynamically updating the per-flow

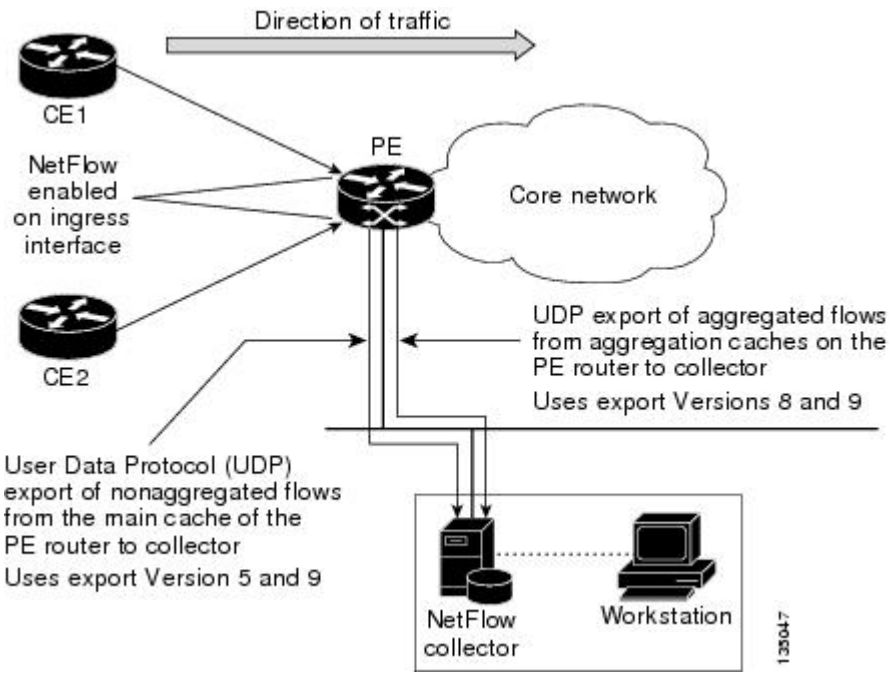
accounting measurements that reside in the NetFlow cache, and determining cache aging or flow expiration.

The rules for expiring NetFlow cache entries include the following:

- Flows that have been idle for a specified time are expired and removed from the cache.
- Long lived flows are expired and removed from the cache. (Flows are not allowed to live for more than 30 minutes by default; the underlying packet conversation remains undisturbed.)
- As the cache becomes full, a number of heuristics are applied to aggressively age groups of flows simultaneously.
- TCP connections that have reached the end of the byte stream (FIN) or have been reset (RST) are expired.

Expired flows are grouped into "NetFlow export" datagrams for export from the NetFlow- enabled device. NetFlow export datagrams can consist of up to 30 flow records for Version 5 or Version 9 flow export. The NetFlow functionality is configured on a per-interface basis. To configure NetFlow export capabilities, you need to specify the IP address and application port number of the Cisco NetFlow or third-party flow collector. The flow collector is a device that provides NetFlow export data filtering and aggregation capabilities. The figure below shows an example of NetFlow data export from the main and aggregation caches to a collector.

Figure 1 NetFlow Data Export from the Main and Aggregation Caches



NetFlow Export Format Versions 9 8 5 and 1

- Overview, page 34
- Details, page 34
- NetFlow Export Version Formats, page 34
- NetFlow Export Packet Header Format, page 35
- NetFlow Flow Record and Export Format Content Information, page 36

- NetFlow Data Export Format Selection, page 40
- NetFlow Version 9 Data Export Format, page 41
- NetFlow Version 8 Data Export Format, page 43
- NetFlow Version 5 Data Export Format, page 44
- NetFlow Version 1 Data Export Format, page 46

Overview

NetFlow exports data in UDP datagrams in one of the following formats: Version 9, Version 8, Version 7, Version 5, or Version 1:

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and Border Gateway Protocol (BGP) next hop. The Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extensible, so you can use the same export format with future features.
- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme.
- Version 5--A later enhanced version that adds BGP-AS information and flow sequence numbers. (Versions 2 through 4 were not released.) This is the most commonly used format.
- Version 1--The initially released export format that is rarely used today. Do not use the Version 1 export format unless the legacy collection system that you are using requires it. Use either the Version 9 export format or the Version 5 export format.

Details

The following sections provide more detailed information on NetFlow Data Export Formats:

NetFlow Export Version Formats

For all export versions, the NetFlow export datagram consists of a header and a sequence of flow records. The header contains information such as sequence number, record count, and system uptime. The flow record contains flow information such as IP addresses, ports, and routing information.

The NetFlow Version 9 export format is the newest NetFlow export format. The distinguishing feature of the NetFlow Version 9 export format is that it is template based. Templates make the record format extensible. This feature allows future enhancements to NetFlow without requiring concurrent changes to the basic flow-record format.

The use of templates with the NetFlow Version 9 export format provides several other key benefits:

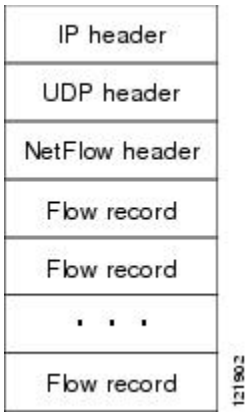
- You can export almost any information from a router or switch, including Layer 2 through 7 information, routing information, and IP Version 6 (IPv6), IP Version 4 (IPv4), Multicast, and MPLS information. This new information allows new applications of export data and provides new views of network behavior.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow export field is added. Instead, they might be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow more quickly, without breaking current implementations.
- Netflow is "future proofed" because the Version 9 export format can be adapted to provide support for new and developing protocols and other non-NetFlow-based approaches to data collection.

The work of the IETF IP, Information Export (IPFIX) Working Group (WG), and the IETF Pack Sampling (PSAMP) WG are based on the NetFlow Version 9 export format.

The Version 1 export format was the original format supported in the initial Cisco IOS software releases containing the NetFlow functionality; it is rarely used today. The Version 5 export format is an enhancement that adds BGP autonomous system information and flow sequence numbers. Versions 2 through 4 and Version 6 export formats were either not released or not supported. The Version 8 export format is the NetFlow export format to use when you enable router-based NetFlow aggregation on Cisco IOS router platforms.

The figure below shows a typical datagram used for NetFlow fixed format export Versions 1, 5, 7, and 8.

Figure 2 Typical Datagram for NetFlow Fixed Format Export Versions 1, 5, 7, 8

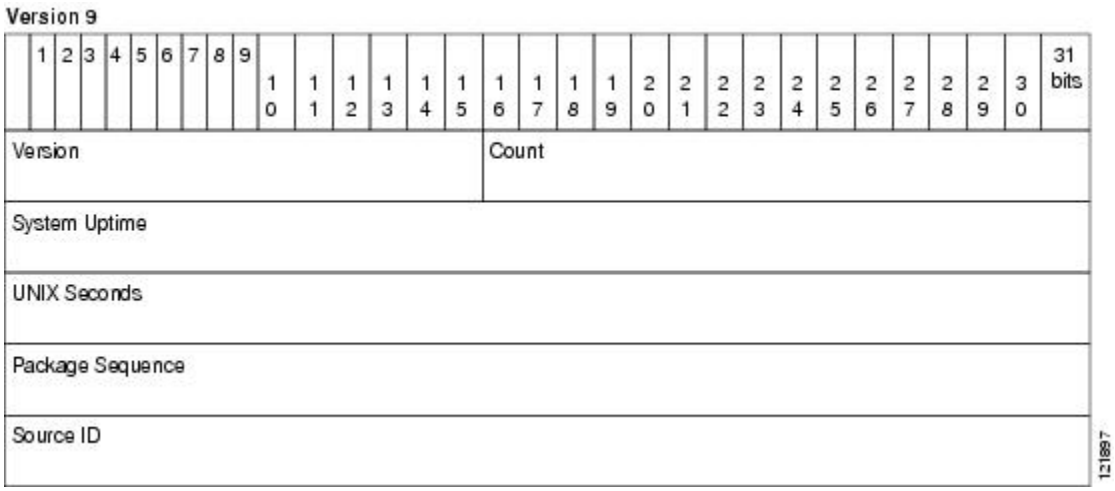


NetFlow Export Packet Header Format

In all the five export versions, the datagram consists of a header and one or more flow records. The first field of the header contains the version number of the export datagram. Typically, a receiving application that accepts any of the format versions allocates a buffer large enough for the largest possible datagram from any of the format versions and then uses the header to determine how to interpret the datagram. The second field in the header contains the number of records in the datagram (indicating the number of expired flows represented by this datagram). Datagram headers for NetFlow Export Versions 5, 8, and 9 also include a "sequence number" field used by NetFlow collectors to check for lost datagrams.

The NetFlow Version 9 export packet header format is shown in the figure below.

Figure 3 NetFlow Version 9 Export Packet Header Format



The table below lists the NetFlow Version 9 export packet header field names and descriptions.

Table 5 NetFlow Version 9 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	The version of NetFlow records exported in this packet; for Version 9, this value is 0x0009.
Count	Number of FlowSet records (both template and data) contained within this packet.
System Uptime	Time in milliseconds since this device was first booted.
UNIX Seconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970.
Package Sequence	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to learn whether any export packets have been missed. This is a change from the NetFlow Version 5 and Version 8 headers, where this number represented "total flows."
Source ID	The Source ID field is a 32-bit value that is used to guarantee uniqueness for each flow exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields found in the NetFlow Version 5 and Version 8 headers.) The format of this field is vendor specific. In Cisco's implementation, the first two bytes are reserved for future expansion and are always zero. Byte 3 provides uniqueness with respect to the routing engine on the exporting device. Byte 4 provides uniqueness with respect to the particular line card or Versatile Interface Processor on the exporting device. Collector devices should use the combination of the source IP address and the Source ID field to associate an incoming NetFlow export packet with a unique instance of NetFlow on a particular device.

NetFlow Flow Record and Export Format Content Information

This section gives details about the Cisco export format flow record. The table below indicates which flow record format fields are available for Versions 5 and 9. ('Yes' indicates that the field is available. 'No' indicates that the field is not available.)

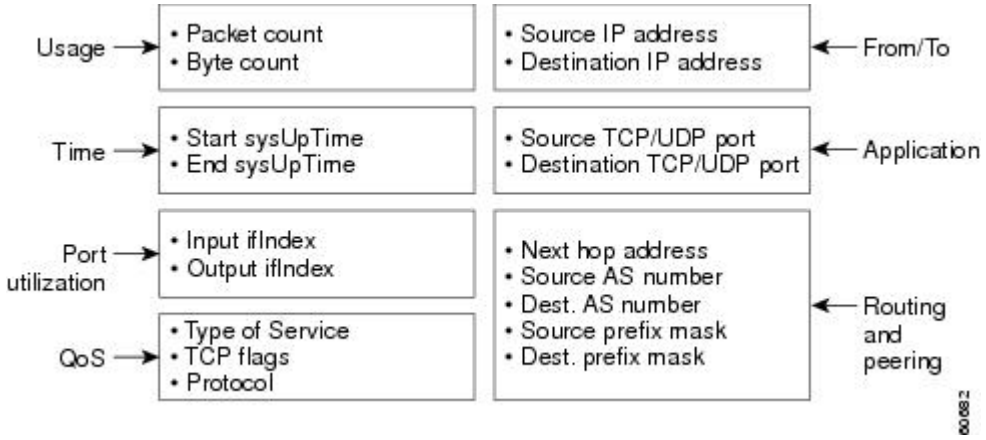
Table 6 NetFlow Flow Record Format Fields for Format Versions 5, and 9

Field	Version 5	Version 9
Source IP address	Yes	Yes
Destination IP address	Yes	Yes
Source TCP/UDP application port	Yes	Yes
Destination TCP/UDP application port	Yes	Yes
Next hop router IP address	Yes	Yes
Input physical interface index	Yes	Yes
Output physical interface index	Yes	Yes
Packet count for this flow	Yes	Yes
Byte count for this flow	Yes	Yes
Start of flow timestamp	Yes	Yes
End of flow timestamp	Yes	Yes
IP Protocol (for example, TCP=6; UDP=17)	Yes	Yes
Type of Service (ToS) byte	Yes	Yes
TCP Flags (cumulative OR of TCP flags)	Yes	Yes
Source AS number	Yes	Yes
Destination AS number	Yes	Yes
Source subnet mask	Yes	Yes
Destination subnet mask	Yes	Yes
Flags (indicates, among other things, which flows are invalid)	Yes	Yes
Other flow fields[1]	No	Yes

1 For a list of other flow fields available in Version 9 export format, see Figure 5 .

The figure below is an example of the NetFlow Version 5 export record format, including the contents and description of byte locations. The terms in **bold** indicate values that were added for the Version 5 format.

Figure 4 NetFlow Version 5 Export Record Format



The table below shows the field names and descriptions for the NetFlow Version 5 export record format.

Table 7 NetFlow Version 5 Export Record Format Field Names and Descriptions

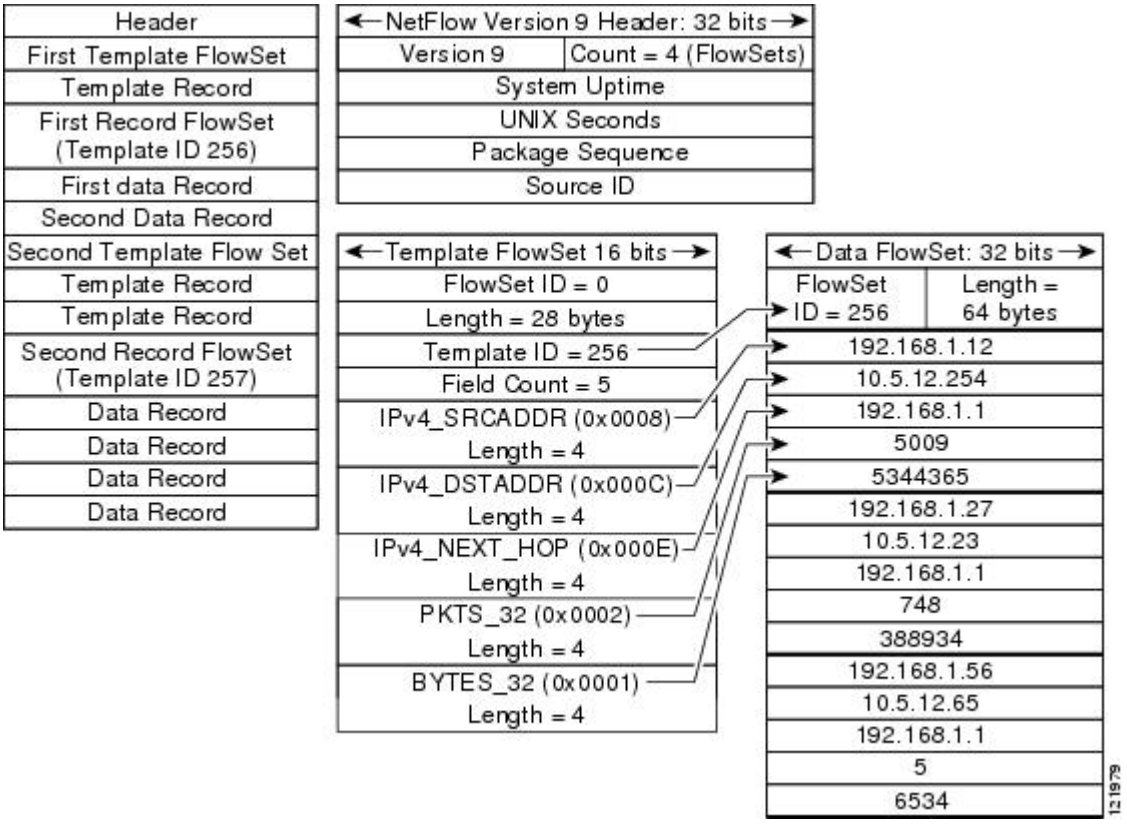
Content	Bytes	Descriptions
srcaddr	0-3	Source IP address
dstaddr	4-7	Destination IP address
nexthop	8-11	Next hop router's IP address
input	12-13	Ingress interface Simple Network Management Protocol (SNMP) ifIndex
output	14-15	Egress interface SNMP ifIndex
dPkts	16-19	Packets in the flow
dOctets	20-23	Octets (bytes) in the flow
first	24-27	SysUptime at start of the flow
last	28-31	SysUptime at the time the last packet of the flow was received
srcport	32-33	Layer 4 source port number or equivalent
dstport	34-35	Layer 4 destination port number or equivalent
pad1	36	Unused (zero) byte

Content	Bytes	Descriptions
tcp_flags	37	Cumulative OR of TCP flags
prot	38	Layer 4 protocol (for example, 6=TCP, 17=UDP)
tos	39	IP type-of-service byte
src_as	40-41	Autonomous system number of the source, either origin or peer
dst_as	42-43	Autonomous system number of the destination, either origin or peer
src_mask	44	Source address prefix mask bits
dst_mask	45	Destination address prefix mask bits
pad2	46-47	PAD2 is unused (zero) bytes

The figure below shows a typical flow record for the Version 9 export format. The NetFlow Version 9 export record format is different from the traditional NetFlow fixed format export record. In NetFlow Version 9, a template describes the NetFlow data and the flow set contains the actual data. This allows for

flexible export. Detailed information about the fields in Version 9 and export format architecture is available in the NetFlow Version 9 Flow-Record Format document.

Figure 5 NetFlow Version 9 Export Packet Example



For all export versions, you can specify a destination where NetFlow data export packets are sent, such as the workstation running NetFlow Collection Engine, when the number of recently expired flows reaches a predetermined maximum, or every second--whichever occurs first. For a Version 1 datagram, up to 24 flows can be sent in a single UDP datagram of approximately 1200 bytes; for a Version 5 datagram, up to 30 flows can be sent in a single UDP datagram of approximately 1500 bytes.

For detailed information on the flow record formats, data types, and export data fields for Versions 1, 7, and 9 and platform-specific information when applicable, see Appendix 2 in the NetFlow Services Solutions Guide .

NetFlow Data Export Format Selection

NetFlow exports data in UDP datagrams in export format Version 9, 8, 5, or 1. The table below describes situations when you might select a particular NetFlow export format.

Table 8 When to Select a Particular NetFlow Export Format

Export Format	Select When...
Version 9	You need to export data from various technologies, such as Multicast, DoS, IPv6, and BGP next hop. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and BGP next hop. The Version 9 export format supports export from the main cache and from aggregation caches.
Version 8	You need to export data from aggregation caches. The Version 8 export format is available only for export from aggregation caches.
Version 5	You need to export data from the NetFlow main cache, and you are not planning to support new features. Version 5 export format does not support export from aggregation caches.
Version 1	You need to export data to a legacy collection system that requires Version 1 export format. Otherwise, do not use Version 1 export format. Use Version 9 or Version 5 export format.

NetFlow Version 9 Data Export Format

The NetFlow Version 9 Export Format feature was introduced in Cisco IOS Release 12.0(24)S and was integrated into Cisco IOS Release 12.3(1) and Cisco IOS Release 12.2(18)S.

NetFlow Version 9 data export supports Cisco Express Forwarding switching, distributed Cisco Express Forwarding switching, and fast switching.

NetFlow Version 9 is a flexible and extensible means for transferring NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

Using Version 9 export, you can define new formats on the router and send these formats to the NetFlow Collection Engine (formerly called NetFlow FlowCollector) at set intervals. You can enable the features that you want, and the field values corresponding to those features are sent to the NetFlow Collection Engine.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow need not recompile their applications each time a new NetFlow technology is added. Instead, with the NetFlow Version 9 Export Format feature, they can use an external data file that documents the known template formats and field types.

In NetFlow Version 9

- Record formats are defined by templates.
- Template descriptions are communicated from the router to the NetFlow Collection Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.

- Version 9 is independent of the underlying transport protocol (UDP, TCP, SCTP, and so on).

NetFlow Version 9 Template-Based Flow Record Format

The main feature of NetFlow Version 9 export format is that it is template based. A template describes a NetFlow record format and attributes of fields (such as type and length) within the record. The router assigns each template an ID, which is communicated to the NetFlow Collection Engine along with the template description. The template ID is used for all further communication from the router to the NetFlow Collection Engine.

NetFlow Version 9 Export Flow Records

The basic output of NetFlow is a flow record. In NetFlow Version 9 export format, a flow record follows the same sequence of fields as found in the template definition. The template to which NetFlow flow records belong is determined by the prefixing of the template ID to the group of NetFlow flow records that belong to a template. For a complete discussion of existing NetFlow flow-record formats, see the NetFlow Services Solutions Guide.

NetFlow Version 9 Export Packet

In NetFlow Version 9, an export packet consists of the packet header and flowsets. The packet header identifies the NetFlow Version 9 Data Export Format, page 41f"> Figure 3 for Version 9 export packet header details. Flowsets are of two types: template flowsets and data flowsets. The template flowset describes the fields that will be in the data flowsets (or flow records). Each data flowset contains the values or statistics of one or more flows with the same template ID. When the NetFlow Collection Engine receives a template flowset, it stores the flowset and export source address so that subsequent data flowsets that match the flowset ID and source combination are parsed according to the field definitions in the template flowset. Version 9 supports NetFlow Collection Engine Version 4.0. For an example of a Version 9 export packet, see NetFlow Version 9 Data Export Format, page 41.

NetFlow Export Templates

NetFlow implements a variety of templates, each exporting a different set of fields for a specific purpose. For example, the MPLS templates are different from the Optimized Edge Routing (OER) templates and the various option templates.

The table below lists the export templates and the specific set of fields the export pertains to.

Table 9 NetFlow Export Templates

Number of Export Templates	Exports Fields Pertaining to...
1	IPv4 main cache
8	MPLS labels 0 to 3
21	Aggregation caches with or without BGP subflows
3	BGP, BGP Next Hop (NH), and Multicast
4	OER
2	MAC and auxiliary information

Number of Export Templates	Exports Fields Pertaining to...
11	Random sampler information, interface names, sampling option, and exporter status options

NetFlow Version 8 Data Export Format

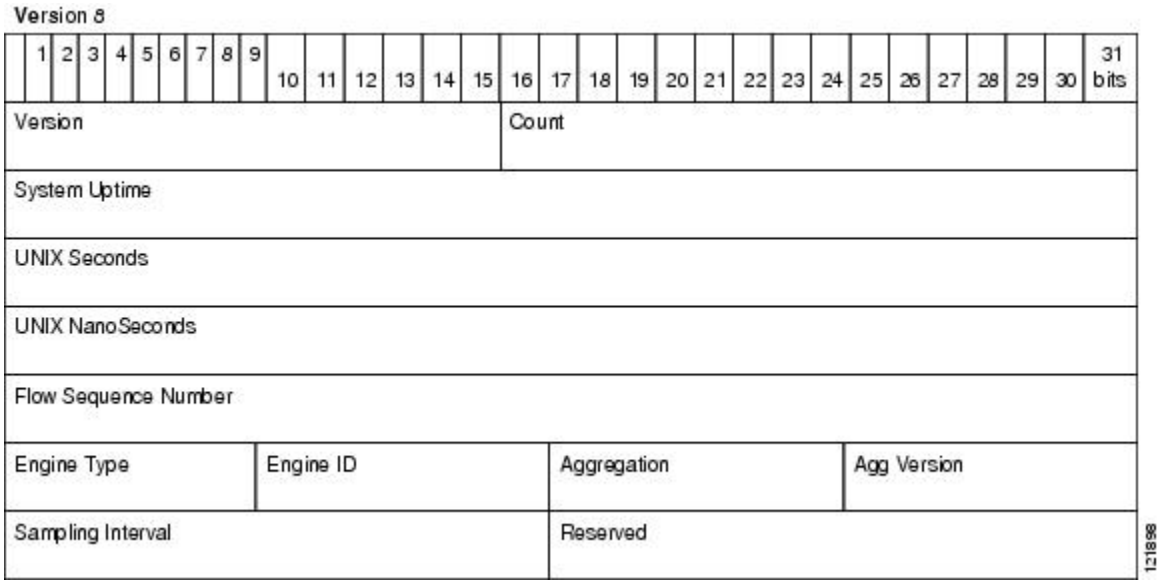
The Version 8 data export format is the NetFlow export format used when the router-based NetFlow Aggregation feature is enabled on Cisco IOS router platforms. The Version 8 format allows for export datagrams to contain a subset of the Version 5 export data that is based on the configured aggregation cache scheme. For example, a certain subset of the Version 5 export data is exported for the destination prefix aggregation scheme, and a different subset is exported for the source-prefix aggregation scheme.

The Version 8 export format was introduced in Cisco IOS Release 12.0(3)T for the Cisco IOS NetFlow Aggregation feature. An additional six aggregation schemes that also use Version 8 format were defined for the NetFlow ToS-Based Router Aggregation feature introduced in Cisco IOS 12.0(15)S and integrated into Cisco IOS Releases 12.2(4)T and 12.2(14)S. Refer to the "Configuring NetFlow Aggregation Caches" module for information on configuring Version 8 data export for aggregation caches.

The Version 8 datagram consists of a header with the version number (which is 8) and time-stamp information, followed by one or more records corresponding to individual entries in the NetFlow cache.

The figure below displays the NetFlow Version 8 export packet header format.

Figure 6 NetFlow Version 8 Export Packet Header Format



The table below lists the NetFlow Version 8 export packet header field names and definitions.

Table 10 NetFlow Version 8 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	Flow export format version number. In this case 8.

Field Name	Description
Count	Number of export records in the datagram.
System Uptime	Number of milliseconds since the router last booted.
UNIX Seconds	Number of seconds since 0000 UTC 1970.
UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
Flow Sequence Number	Sequence counter of total flows sent for this export stream.
Engine Type	The type of switching engine. RP = 0 and LC = 1.
Engine ID	Slot number of the NetFlow engine.
Aggregation	Type of aggregation scheme being used.
Agg Version	Aggregation subformat version number. The current value is 2.
Sampling Interval	Interval value used if Sampled NetFlow is configured.
Reserved	Reserved.

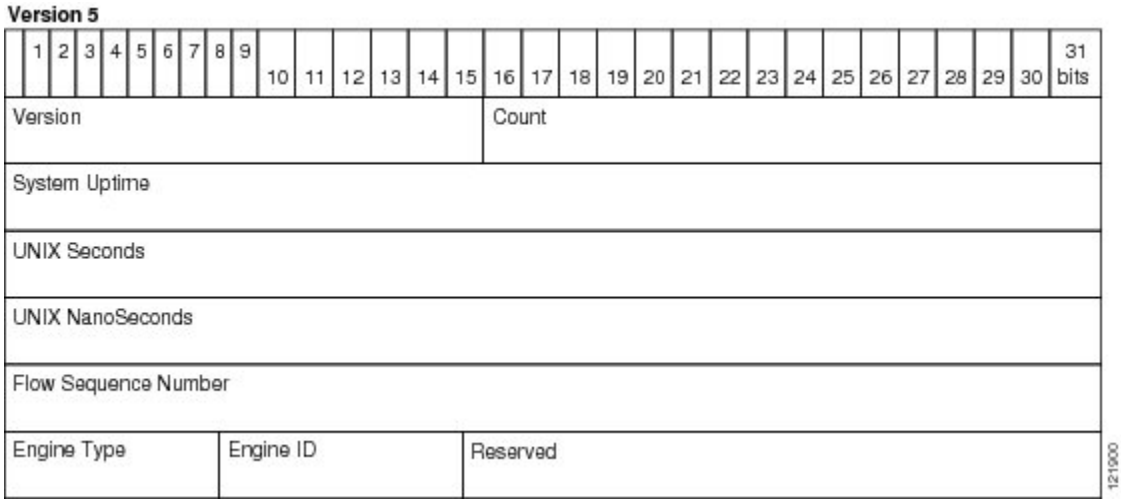
NetFlow Version 5 Data Export Format

The Version 5 data export format adds support for BGP autonomous system information and flow sequence numbers.

Because NetFlow uses UDP to send export datagrams, datagrams can be lost. The Version 5 header format contains a flow sequence number to find out whether flow export information has been lost. The sequence number is equal to the sequence number of the previous datagram plus the number of flows in the previous datagram. After receiving a new datagram, the receiving application can subtract the expected sequence number from the sequence number in the header to get the number of missed flows.

All fields in the Version 5 export format are in network byte order. The figure below shows the NetFlow Version 5 export packet header format.

Figure 7 NetFlow Version 5 Export Packet Header Format



The table below lists the NetFlow Version 5 export packet header field names and descriptions.

Table 11 NetFlow Version 5 Export Packet Header Field Names and Descriptions

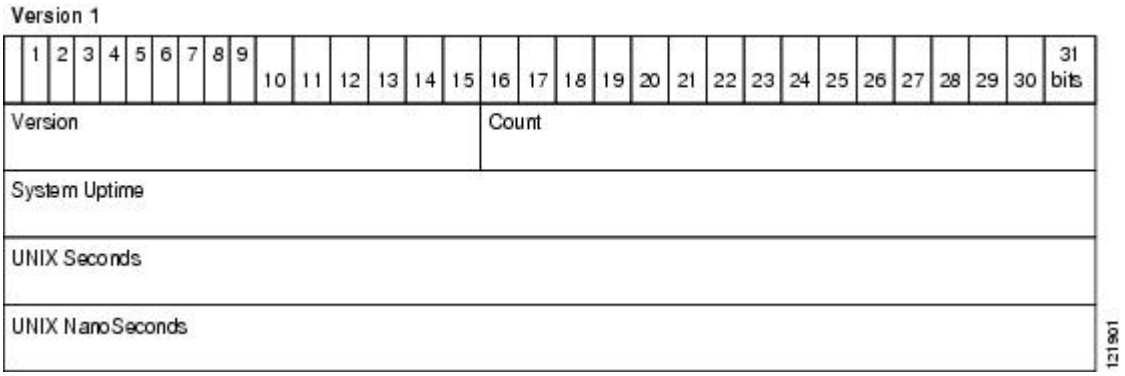
Bytes	Field	Description
0 to 1	Version	Flow export format version number. In this case 5.
2 to 3	Count	Number of export records in the datagram.
4 to 7	System Uptime	Number of milliseconds since the router last booted.
8 to 11	UNIX Seconds	Number of seconds since 0000 UTC 1970.
12 to 15	UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
16 to 19	Flow Sequence Number	Sequence counter of total flows sent for this export stream.
20	Engine Type	The type of switching engine. RP = 0 and LC = 1.
21	Engine ID	Slot number of the NetFlow engine.
22 to 23	Reserved	Reserved.

NetFlow Version 1 Data Export Format

The NetFlow Version 1 data export format was the format supported in the initial Cisco IOS software releases containing the NetFlow functionality. It is rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format.

The figure below shows the NetFlow Version 1 export packet header format.

Figure 8 Version 1 Export Packet Header Format



The table below lists the NetFlow Version 1 export packet header field names and descriptions.

Table 12 NetFlow Version 1 Packet Header Field Names and Descriptions

Field Name	Description
Version	Flow export format version number. In this case 1.
Count	Number of export records in the datagram.
System Uptime	Number of milliseconds since the router last booted.
UNIX Seconds	Number of seconds since 0000 UTC 1970.
UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.

Egress NetFlow Accounting Benefits NetFlow Accounting Simplified

The Egress NetFlow Accounting feature can simplify the NetFlow configuration. The following example shows how.

In the two figures below, both incoming and outgoing (ingress and egress) flow statistics are required for the server. The server is attached to Router B. The "cloud" in the figure represents the core of the network and includes MPLS VPNs.

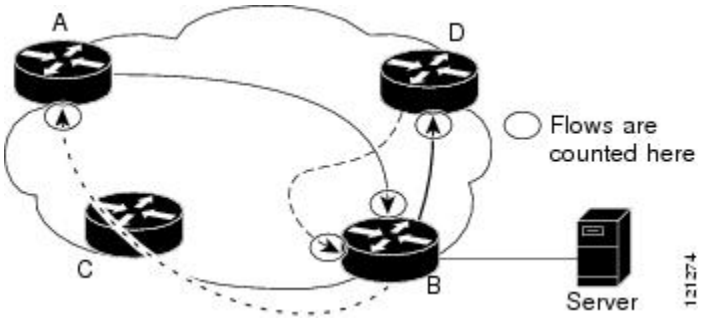
All traffic denoted by the arrows must be accounted for. The solid arrows represent IP traffic and the dotted arrows represent MPLS VPNs.

The first figure below shows how the flow traffic was tracked before the introduction of the Egress NetFlow Accounting feature. The second figure below shows how the flow traffic is tracked after the introduction of the Egress NetFlow Accounting feature. The Egress NetFlow Accounting feature simplifies configuration tasks and facilitates collection and tracking of incoming and outgoing flow statistics for the server in this example.

Because only ingress flows could be tracked before the Egress NetFlow Accounting feature was introduced, the following NetFlow configurations had to be implemented for the tracking of ingress and egress flows from Router B:

- Enable NetFlow on an interface on Router B to track ingress IP traffic from Router A to Router B.
- Enable NetFlow on an interface on Router D to track ingress IP traffic from Router B to Router D.
- Enable NetFlow on an interface on Router A to track ingress traffic from the MPLS VPN from Router B to Router A.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router D to Router B.

Figure 9 Ingress-Only NetFlow Example



A configuration such as the one used in the figure above requires that NetFlow statistics from three separate routers be added to obtain the flow statistics for the server.

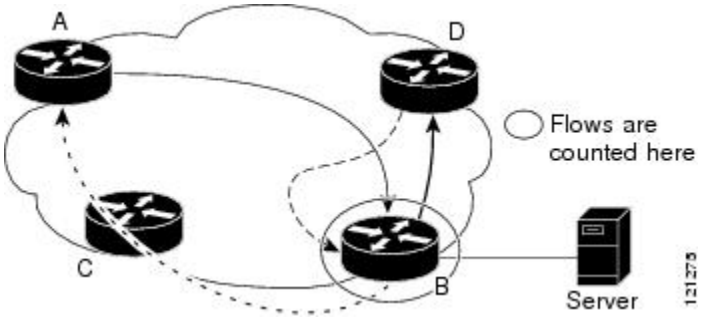
In comparison, the example in the figure below shows NetFlow, the Egress NetFlow Accounting feature, and the MPLS Egress NetFlow Accounting feature being used to capture ingress and egress flow statistics for Router B, thus obtaining the required flow statistics for the server.

In the figure below, the following NetFlow configurations are applied to Router B:

- Enable NetFlow on an interface on Router B to track ingress IP traffic from Router A to Router B.
- Enable the Egress NetFlow Accounting feature on an interface on Router B to track egress IP traffic from Router B to Router D.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router B to Router D.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router B to Router A.

After NetFlow is configured on Router B, you can display all NetFlow statistics for the server by using the **show ip cache flow** command or the **show ip cache verbose flow** command for Router B.

Figure 10 Egress NetFlow Accounting Example



NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection

You can configure NetFlow on a per-subinterface basis. If your network contains thousands of subinterfaces, you can collect export records from just a few of them. The result is lower bandwidth requirements for NetFlow data export and reduced platform requirements for NetFlow data-collection devices.

The configuration of NetFlow on selected subinterfaces provides the following benefits:

- Reduced bandwidth requirement between routing devices and NetFlow management workstations.
- Reduced NetFlow workstation requirements; the number of flows sent to the workstation for processing is reduced.

NetFlow Multiple Export Destinations Benefits

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations for the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data because it provides redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets are lost.

NetFlow on a Distributed VIP Interface

On a Cisco 7500 series router with a Route Switch Processor (RSP) and with VIP controllers, the VIP hardware can be configured to switch packets received by the VIP interfaces with no per-packet intervention on the part of the RSP. This process is called distributed switching. When VIP distributed switching is enabled, the input VIP interface switches IP packets instead of forwarding them to the RSP for switching. Distributed switching decreases the demand on the RSP. VIP interfaces with distributed switching enabled can be configured for NetFlow.

How to Configure NetFlow and NetFlow Data Export

This section contains instructions for configuring NetFlow to capture and export network traffic data. Perform the following tasks to configure NetFlow to capture and export network traffic data:

- Configuring NetFlow, page 48
- Verifying that NetFlow Is Operational and Displaying NetFlow Statistics, page 50
- Configuring NetFlow Data Export Using the Version 9 Export Format, page 52
- Verifying that NetFlow Data Export Is Operational, page 55
- Clearing NetFlow Statistics on the Router, page 56
- Customizing the NetFlow Main Cache Parameters, page 57

Configuring NetFlow

Perform the following task to enable NetFlow on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces.
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 4	**ip flow** {**ingress**	**egress**} **Example:** `Router(config-if)# ip flow ingress` **Example:**	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and enters global configuration mode. **Note** You need to use this command only if you want to enable NetFlow on another interface.

	Command or Action	Purpose
Step 6	Repeat Steps 3 through 5 to enable NetFlow on other interfaces.	This step is optional.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying that NetFlow Is Operational and Displaying NetFlow Statistics

Perform the following task to verify that NetFlow is operational and to display NetFlow statistics.

SUMMARY STEPS

1. **show ip flow interface**
2. **show ip cache flow**
3. **show ip cache verbose flow**

DETAILED STEPS

Step 1 **show ip flow interface**

Use this command to display the NetFlow configuration for an interface. The following is sample output from this command:

Example:

```
Router# show ip flow interface

Ethernet0/0
  ip flow ingress
Router#
```

Step 2 **show ip cache flow**

Use this command to verify that NetFlow is operational and to display a summary of NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
```

```
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.8    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.1    1799.6       0.9
ICMP               135      0.0      1133   427      3.1    1799.6       0.8
Total:             945      0.0      1166    91     22.4    1799.6       0.8
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.67.6    Et1/0.1       172.16.10.200   01 0000 0C01    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0043 0043    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0045 0045    51
Et0/0         10.234.53.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 0044 0044    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 00A2 00A2    51
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0014 0014    50
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0015 0015    52
.
.
.
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0087 0087    50
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0050 0050    51
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0089 0089    49
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0050 0050    50
Et0/0         10.251.10.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.162.37.71    Null          172.16.11.3     06 027C 027C    49
Router#
```

Step 3 **show ip cache verbose flow**

Use this command to verify that NetFlow is operational and to display a detailed summary of NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (1130681 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2992518 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.6    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
```

```
UDP-other          108      0.0      1417    28      3.0    1799.6       0.9
ICMP               135      0.0      1133   427      3.0    1799.6       0.8
Total:             945      0.0      1166    91     21.9    1799.6       0.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0          192.168.67.6    Et1/0.1        172.16.10.200   01 00  10     799
0000 /0  0                     0C01 /0  0     0.0.0.0                 28  1258.1
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0043 /0  0                     0043 /0  0     0.0.0.0                 28  1258.0
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0045 /0  0                     0045 /0  0     0.0.0.0                 28  1258.0
Et0/0          10.234.53.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0                 28  1258.1
Et0/0          10.10.19.1      Null           172.16.11.6     11 00  10     799
0044 /0  0                     0044 /0  0     0.0.0.0                 28  1258.1
.
.
.
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0087 /0  0                     0087 /0  0     0.0.0.0                 40  1258.1
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                 40  1258.0
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     798
0089 /0  0                     0089 /0  0     0.0.0.0                 40  1256.5
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                 40  1258.0
Et0/0          10.251.10.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0               1500  1258.1
Et0/0          10.162.37.71    Null           172.16.11.3     06 00  00     798
027C /0  0                     027C /0  0     0.0.0.0                 40  1256.4
Router#
```

Configuring NetFlow Data Export Using the Version 9 Export Format

Perform the steps in this optional task to configure NetFlow Data Export using the Version 9 export format.

Note This task does not include instructions for configuring Reliable NetFlow Data Export using the Stream Control Transmission Protocol (SCTP). Refer to the NetFlow Reliable Export with SCTP module for information about and instructions for configuring Reliable NetFlow Data Export using SCTP.

This task does not include the steps for configuring NetFlow. You must configure NetFlow by enabling it on at least one interface in the router in order to export traffic data with NetFlow Data Export. Refer to the Configuring NetFlow, page 48 for information about configuring NetFlow.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*
4. Repeat Step 3 once to configure an additional NetFlow export destination.
5. **ip flow-export source** *interface-type interface-number*
6. **ip flow-export version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**]
7. **ip flow-export interface-names**
8. **ip flow-export template refresh-rate** *packets*
9. **ip flow-export template timeout-rate** *minutes*
10. **i p flow-export template options export-stats**
11. **ip flow-export template options refresh-rate** *packets*
12. **ip flow-export template options timeout-rate** *minutes*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	Specifies the IP address, or hostname of the NetFlow collector, and the UDP port the NetFlow collector is listening on.
Step 4	Repeat Step 3 once to configure an additional NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.

	Command or Action	Purpose
Step 5	**ip flow-export source** *interface-type interface-number* **Example:** `Router(config)# ip flow-export source ethernet 0/0`	(Optional) Specifies the IP address from the interface. The IP address is used as the source IP address for the UDP datagrams that are sent by NetFlow data export to the destination host.
Step 6	**ip flow-export version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**] **Example:** `Router(config)# ip flow-export version 9`	(Optional) Enables the export of information in NetFlow cache entries. • The **version 9** keyword specifies that the export packet uses the Version 9 format. • The **origin-as** keyword specifies that export statistics include the originating autonomous system for the source and destination. • The **peer-as** keyword specifies that export statistics include the peer autonomous system for the source and destination. • The **bgp-nexthop** keyword specifies that export statistics include BGP next hop-related information. **Caution** Entering this command on a Cisco 12000 series Internet router causes packet forwarding to stop for a few seconds while NetFlow reloads the RP and LC Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 7	**ip flow-export interface-names** **Example:** `Router(config)# ip flow-export interface-names`	Configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.
Step 8	**ip flow-export template refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template refresh-rate 15` **Example:**	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are re-sent. You can specify from 1 to 600 packets. The default is 20.

	Command or Action	Purpose
Step 9	**ip flow-export template timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template timeout-rate 90`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies that the **timeout-rate** keyword applies to the template. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are re-sent. You can specify from 1 to 3600 minutes. The default is 30.
Step 10	**i p flow-export template options export-stats** **Example:** `Router(config)# ip flow-export template options export-stats`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **export-stats**keyword specifies that the export statistics include the total number of flows exported and the total number of packets exported.
Step 11	**ip flow-export template options refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template options refresh-rate 25`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are re-sent. You can specify from 1 to 600 packets. The default is 20.
Step 12	**ip flow-export template options timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template options timeout-rate 120`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are re-sent. You can specify from 1 to 3600 minutes. The default is 30.
Step 13	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and enters privileged EXEC mode.

Verifying that NetFlow Data Export Is Operational

Perform the steps in this optional task to verify that NetFlow data export is operational and to display the statistics for NetFlow data export.

SUMMARY STEPS

1. **show ip flow export**
2. **show ip flow export template**

DETAILED STEPS

Step 1 **show ip flow export**

Use this command to display statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

Example:

```
Router# show ip flow export
Flow export v9 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source interface Ethernet0/0
  Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Step 2 **show ip flow export template**

Use this command to display statistics for the NetFlow data export (such as the template timeout rate and the refresh rate) for template-specific configurations. The following is sample output from this command:

Example:

```
Router# show ip flow export template
   Template Options Flag = 1
   Total number of Templates added = 1
   Total active Templates = 1
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 1
   Option  Templates added = 1
   Template ager polls = 0
   Option Template ager polls = 140
Main cache version 9 export is enabled
 Template export information
   Template timeout = 90
   Template refresh rate = 15
 Option export information
   Option timeout = 120
   Option refresh rate = 25
Router#
```

Clearing NetFlow Statistics on the Router

Perform the steps in this optional task to clear NetFlow statistics on the router.

SUMMARY STEPS

1. **enable**
2. **clear ip flow stats**

DETAILED STEPS

Step 1 **enable**
Use this command to enter privileged EXEC mode on the router:

Example:

```
Router> enable
Router#
```

Step 2 **clear ip flow stats**
Use this command to clear the NetFlow statistics on the router. For example:

Example:

```
Router# clear ip flow stats
```

Customizing the NetFlow Main Cache Parameters

NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. A flow record is maintained within the NetFlow cache for all active flows. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine. NetFlow enables the accumulation of data on flows. Each flow is identified by unique characteristics such as the IP address, interface, application, and ToS.

To customize the parameters for the main NetFlow cache, perform the steps in this optional task.

- NetFlow Cache Entry Management on a Routing Device, page 57
- NetFlow Cache Size, page 58

NetFlow Cache Entry Management on a Routing Device

The routing device checks the NetFlow cache once per second and causes the flow to expire in the following instances:

- Flow transport is completed (TCP connections that have reached the end of the byte stream [FIN] or that have been reset [RST] are expired).
- The flow cache has become full.
- A flow becomes inactive. By default, a flow that is unaltered in the last 15 seconds is classified as inactive.
- An active flow has been monitored for a specified number of minutes. By default, active flows are flushed from the cache when they have been monitored for 30 minutes.

Routing device default timer settings are 15 seconds for the inactive timer and 30 minutes for the active timer. You can configure your own time interval for the inactive timer from 10 to 600 seconds. You can configure the time interval for the active timer from 1 to 60 minutes.

NetFlow Cache Size

After you enable NetFlow on an interface, NetFlow reserves memory to accommodate a number of entries in the NetFlow cache. Normally, the size of the NetFlow cache meets the needs of your NetFlow traffic rates. The cache default size is 64K flow cache entries. Each cache entry requires 64 bytes of storage. About 4 MB of DRAM are required for a cache with the default number of entries. You can increase or decrease the number of entries maintained in the cache, if required. For environments with a large amount of flow traffic (such as an Internet core router), Cisco recommends a larger value such as 131072 (128K). To obtain information on your flow traffic, use the **show ip cache flow command.**

A NetFlow cache can be resized depending on the platform and the amount of DRAM on a line card. For example, the NetFlow cache size is configurable for software-based platforms such as Cisco 75xx and 72xx series routers. The amount of memory on a Cisco 12000 line card determines how many flows are possible in the cache.

Using the **ip flow-cache entries** command, configure the size of your NetFlow cache from 1024 entries to 524,288 entries. Use the **cache entries** command (after you configure NetFlow aggregation) to configure the size of the NetFlow aggregation cache from 1024 entries to 524,288 entries.

Caution Cisco recommends that you not change the values for NetFlow cache entries. Improper use of this feature could cause network problems. To return to the default value for NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Note If you modify any parameters for the NetFlow main cache after you enable NetFlow, the changes will not take effect until you reboot the router or disable NetFlow on every interface it is enabled on, and then re-enable NetFlow on the interfaces.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 for every interface that has NetFlow enabled on it.
7. **ip flow-cache entries** *number*
8. **ip flow-cache timeout active** *minutes*
9. **ip flow-cache timeout inactive** *seconds*
10. **interface** *type number*
11. **ip flow** {**ingress** | **egress**}
12. **exit**
13. Repeat Steps 10 through 12 for every interface that previously had NetFlow enabled on it.
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	(Required if NetFlow is already enabled on the interface) Specifies the interface that you want to disable NetFlow on and enters interface configuration mode.
Step 4	**no ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# no ip flow ingress` **Example:**	(Required if NetFlow is enabled on the interface) Disables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you need to disable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 for every interface that has NetFlow enabled on it.	This step is required if NetFlow is enabled on any other interfaces. --
Step 7	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 131072`	(Optional) Changes the number of entries maintained in the NetFlow cache. • The *number* argument is the number of entries to be maintained. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).

	Command or Action	Purpose
Step 8	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 20`	(Optional) Specifies flow cache timeout parameters. • The **active** keyword specifies the active flow timeout. • The *minutes* argument specifies the number of minutes that an active flow remains in the cache before the flow times out. The range is from 1 to 60. The default is 30.
Step 9	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 130`	(Optional) Specifies flow cache timeout parameters. • The **inactive** keyword specifies the inactive flow timeout. • The *seconds* argument specifies the number of seconds that an inactive flow remains in the cache before it times out. The range is from 10 to 600. The default is 15.
Step 10	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 11	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress` **Example:**	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface
Step 12	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You need to use this command only if you need to enable NetFlow on another interface.
Step 13	Repeat Steps 10 through 12 for every interface that previously had NetFlow enabled on it.	This step is required for any other interfaces that you need to enable NetFlow on.
Step 14	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and enters privileged EXEC mode.

Configuration Examples for Configuring NetFlow and NetFlow Data Export

- Example Configuring Egress NetFlow Accounting, page 61
- Example Configuring NetFlow Subinterface Support, page 61
- Example Configuring NetFlow Multiple Export Destinations, page 62
- Example Configuring NetFlow Version 5 Data Export, page 62
- Example Configuring NetFlow Version 1 Data Export, page 63

Example Configuring Egress NetFlow Accounting

The following example shows how to configure Egress NetFlow Accounting as described in the Egress NetFlow Accounting Benefits NetFlow Accounting Simplified, page 46:

```
configure terminal
!
interface ethernet 0/0
 ip flow egress
!
```

Example Configuring NetFlow Subinterface Support

The following examples show how to configure NetFlow Subinterface Support as described in the NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection, page 48:

- NetFlow Subinterface Support for Ingress (Received) Traffic on a Subinterface, page 61
- NetFlow SubInterface Support for Egress (Transmitted) Traffic on a Subinterface, page 61

NetFlow Subinterface Support for Ingress (Received) Traffic on a Subinterface

```
configure terminal
!
interface ethernet 0/0.1
 ip flow ingress
!
```

NetFlow SubInterface Support for Egress (Transmitted) Traffic on a Subinterface

```
configure terminal
!
interface ethernet 1/0.1
 ip flow egress
!
```

Note NetFlow performs additional checks for the status of each subinterface that requires more CPU processing time and bandwidth. If you have several subinterfaces configured and you want to configure NetFlow data capture on all of them, we recommend that you configure NetFlow on the main interface instead of on the individual subinterfaces.

Example Configuring NetFlow Multiple Export Destinations

The following example shows how to configure the NetFlow Multiple Export Destinations feature as described in the NetFlow Multiple Export Destinations Benefits, page 48:

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export destination 172.16.10.2 9991
!
```

Note You can configure a maximum of two export destinations for the main cache and for each aggregation cache.

Example Configuring NetFlow Version 5 Data Export

The following example shows how to configure the NetFlow data export using the Version 5 export format with the peer autonomous system information:

```
configure terminal

!

ip flow-export version 5 peer-as
ip flow-export destination 172.16.10.2 99
exit
Router# show ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source IP address 172.16.6.1
  Version 5 flow records, peer-as
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Example Configuring NetFlow Version 1 Data Export

The following example shows how to configure the NetFlow data export using the Version 5 export format with the peer autonomous system information:

```
configure terminal

!

ip flow-export destination 172.16.10.2 99
exit
Router# show ip flow export
Flow export v1 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source IP address 172.16.6.1
  Version 1 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Note No autonomous system number or BGP next hop information is exported with the Version 1 export format.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NetFlow Commands	*Cisco IOS NetFlow Command Reference*
NetFlow Version 9 Flow-Record Format	NetFlow Version 9 Flow-Record Format
NetFlow Services Solutions Guide	*NetFlow Services Solutions Guide*
NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring NetFlow and NetFlow Data Export

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13 Feature Information for Configuring NetFlow and NetFlow Data Export

Feature Name	Releases	Feature Information
Egress NetFlow Accounting	12.3(11)T 15.0(1)S	The Egress NetFlow Accounting feature allows NetFlow statistics to be gathered on egress traffic that is exiting the router. Previous versions of NetFlow allow statistics to be gathered only on ingress traffic that is entering the router. The following commands were introduced by this feature: **ip flow egress** and **ip flow-egress input-interface**. The following commands were modified by this feature: **flow-sampler**, **match**, **show ip cache flow**, **show ip cache verbose flow**, and **show ip flow interface**.
NetFlow Multiple Export Destinations	12.0(19)S 12.2(2)T 12.2(14)S 15.0(1)S	The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. The following commands were modified by this feature: **ip flow-aggregation cache**, **ip flow-export destination**, and **show ip flow export**.
NetFlow Subinterface Support	12.0(22)S 12.2(14)S 12.2(15)T 12.2(33)SB	The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. The following command was introduced by this feature: **ip flow ingress.** The following command was modified by this feature: **show ip interface**.

Feature Name	Releases	Feature Information
NetFlow v9 Export Format	12.0(24)S 12.2(18)S 12.2(27)SBC 12.2(18)SXF 12.3(1) 15.0(1)S	The NetFlow v9 Export Format, which is flexible and extensible, provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, NAT, and BGP next hop. The following commands were modified by this feature: **debug ip flow export**, **export**, **ip flow-export**, and **show ip flow export**.
Support for interface names added to NetFlow data export[2]	12.4(2)T	The **interface-names** keyword for the **ip flow-export** command configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.

Glossary

Autonomous system--A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

Cisco Express Forwarding--A layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used by a router to reach a certain destination.

distributed Cisco Express Forwarding--A type of Cisco Express Forwarding switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the Forwarding Information Base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --Type of packet built by a NetFlow-services-enabled device (for example, a router) that is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes (parses, aggregates, and stores information on IP flows) the packet.

fast switching --A Cisco feature in which a route cache is used to expedite packet switching through a router.

2 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type of service, and with the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

MPLS --Multiprotocol Label Switching. An industry standard for the forwarding of packets along a normally routed path (sometimes called MPLS hop-by-hop forwarding).

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on a Cisco IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

RP --Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a Supervisory Processor.

Configuring NetFlow Aggregation Caches

This module contains information about and instructions for configuring NetFlow aggregation caches. The NetFlow main cache is the default cache used to store the data captured by NetFlow. By maintaining one or more extra caches, called aggregation caches, the NetFlow Aggregation feature allows limited aggregation of NetFlow data export streams on a router. The aggregation scheme that you select determines the specific kinds of data that are exported to a remote host.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

- Finding Feature Information, page 69
- Prerequisites for Configuring NetFlow Aggregation Caches, page 69
- Restrictions for Configuring NetFlow Aggregation Caches, page 70
- Information About Configuring NetFlow Aggregation Caches, page 71
- How to Configure NetFlow Aggregation Caches, page 92
- Configuration Examples for Configuring NetFlow Aggregation Caches, page 98
- Additional References, page 102
- Feature Information for Configuring NetFlow Aggregation Caches, page 104
- Glossary, page 105

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring NetFlow Aggregation Caches

Before you enable NetFlo, you must:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources

If you intend to use Version 8 export format with an aggregation cache, configure Version 5 export format for the main cache.

If you need autonomous system (AS) information from the aggregation, make sure to specify either the **peer-as**or **origin-as** keyword in your export command if you have not configured an export format version.

You must explicitly enable each NetFlow aggregation cache by entering the **enabled** keyword from aggregation cache configuration mode.

Router-based aggregation must be enabled for minimum masking.

Restrictions for Configuring NetFlow Aggregation Caches

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface.

Memory Impact

During times of heavy traffic, the additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Performance Impact

Configuring Egress NetFlow accounting with the **ip flow egress** command might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

- NetFlow Data Export, page 70

NetFlow Data Export

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets) versus Version 5. The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

Restrictions for NetFlow Version 8 Export Format

Version 8 export format is available only for aggregation caches, and it cannot be expanded to support new features.

Information About Configuring NetFlow Aggregation Caches

- NetFlow Aggregation Caches, page 71
- NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview, page 92

NetFlow Aggregation Caches

- NetFlow Cache Aggregation Benefits, page 71
- NetFlow Cache Aggregation Schemes, page 71
- NetFlow Aggregation Scheme Fields, page 73
- NetFlow AS Aggregation Scheme, page 75
- NetFlow AS-ToS Aggregation Scheme, page 76
- NetFlow Destination Prefix Aggregation Scheme, page 78
- NetFlow Destination Prefix-ToS Aggregation Scheme, page 79
- NetFlow Prefix Aggregation Scheme, page 81
- NetFlow Prefix-Port Aggregation Scheme, page 82
- NetFlow Prefix-ToS Aggregation Scheme, page 84
- NetFlow Protocol Port Aggregation Scheme, page 86
- NetFlow Protocol-Port-ToS Aggregation Scheme, page 87
- NetFlow Source Prefix Aggregation Scheme, page 89
- NetFlow Source Prefix-ToS Aggregation Scheme, page 90

NetFlow Cache Aggregation Benefits

Aggregation of export data is typically performed by NetFlow collection tools on management workstations. Router-based aggregation allows limited aggregation of NetFlow export records to occur on the router. Thus, you can summarize NetFlow export data on the router before the data is exported to a NetFlow data collection system, which has the following benefits:

- Reduces the bandwidth required between the router and the workstations
- Reduces the number of collection workstations required
- Improves performance and scalability on high flow-per-second routers

NetFlow Cache Aggregation Schemes

Cisco IOS NetFlow aggregation maintains one or more extra caches with different combinations of fields that determine which flows are grouped together. These extra caches are called aggregation caches. The combinations of fields that make up an aggregation cache are referred to as schemes. As flows expire from the main cache, they are added to each enabled aggregation cache.

You can configure each aggregation cache with its individual cache size, cache ager timeout parameter, export destination IP address, and export destination UDP port. As data flows expire in the main cache (depending on the aggregation scheme configured), relevant information is extracted from the expired flow and the corresponding flow entry in the aggregation cache is updated. The normal flow ager process runs on each active aggregation cache the same way it runs on the main cache. On-demand aging is also

supported. Each aggregation cache contains different field combinations that determine which data flows are grouped. The default aggregation cache size is 4096 bytes.

You configure a cache aggregation scheme through the use of arguments to the **ip flow-aggregation cache** command. NetFlow supports the following five non-ToS based cache aggregation schemes:

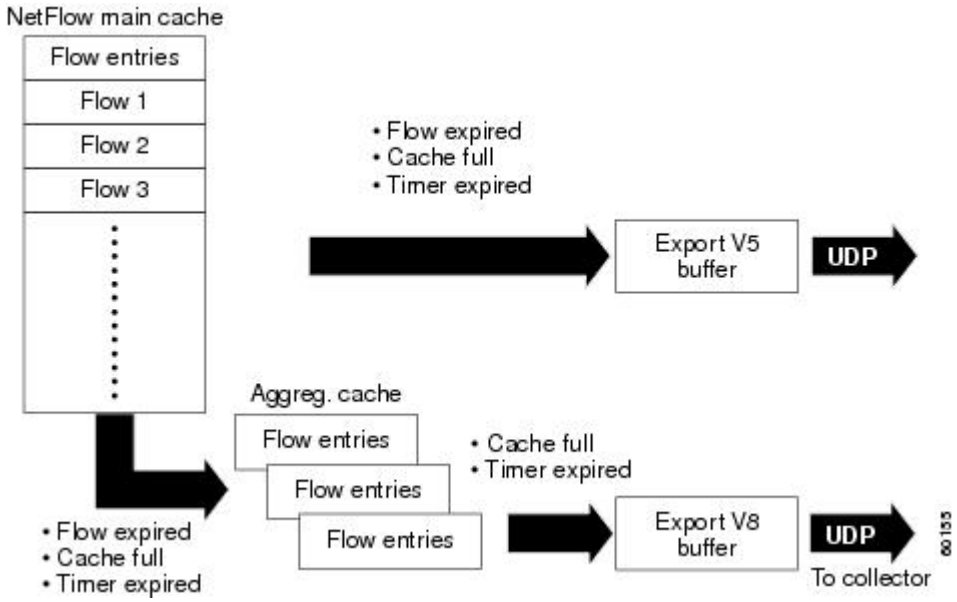
- Autonomous system (AS) aggregation scheme
- Destination prefix aggregation scheme
- Prefix aggregation scheme
- Protocol port aggregation scheme
- Source prefix aggregation scheme

The NetFlow Type of Service (ToS)-Based Router Aggregation feature introduced support for additional cache aggregation schemes, all of which include the ToS byte as one of the fields in the aggregation cache. The following are the six ToS-based aggregation schemes:

- AS-ToS aggregation scheme
- Destination prefix-ToS aggregation scheme
- Prefix-port aggregation scheme
- Prefix-ToS aggregation scheme
- Protocol-port-ToS aggregation scheme
- Source prefix-ToS aggregation scheme

The figure below shows an example of how the main NetFlow cache can be aggregated into multiple aggregation caches based upon user-configured aggregation schemes.

Figure 11 Building a NetFlow Aggregation Cache



Note NetFlow Aggregation Scheme Fields, page 73 through NetFlow Cache Aggregation Schemes, page 71 illustrate the Version 8 export formats of the aggregation schemes listed above. Additional export formats (for instance, Version 9) are also supported. If you are using Version 9, the formats will be different from those shown in the figures. For more information about Version 9 export formats, see Configuring NetFlow and NetFlow Data Export.

NetFlow Aggregation Scheme Fields

Each cache aggregation scheme contains field combinations that differ from any other cache aggregation scheme. The combination of fields determines which data flows are grouped and collected when a flow expires from the main cache. A flow is a set of packets that has common fields, such as the source IP address, destination IP address, protocol, source and destination ports, type-of-service, and the same interface on which the flow is monitored. To manage flow aggregation on your router, you need to configure the aggregation cache scheme that groups and collects the fields from which you want to examine data. The tables below show the NetFlow fields that are grouped and collected for non-ToS and ToS based cache aggregation schemes.

The table below shows the NetFlow fields used in the non-TOS based aggregation schemes.

Table 14 NetFlow Fields Used in the Non-ToS Based Aggregations Schemes

Field	AS	Protocol Port	Source Prefix	Destination Prefix	Prefix
Source prefix			X		X
Source prefix mask			X		X
Destination prefix				X	X
Destination prefix mask				X	X
Source app port		X			
Destination app port		X			
Input interface	X		X		X
Output interface	X			X	X
IP protocol		X			
Source AS	X		X		X
Destination AS	X			X	X

Field	AS	Protocol Port	Source Prefix	Destination Prefix	Prefix
First time stamp	X	X	X	X	X
Last time stamp	X	X	X	X	X
Number of flows	X	X	X	X	X
Number of packets	X	X	X	X	X
Number of bytes	X	X	X	X	X

The table below shows the NetFlow fields used in the TOS based aggregation schemes.

Table 15 NetFlow Fields Used in the ToS Based Aggregation Schemes

Field	AS-ToS	Protocol Port-ToS	Source Prefix-ToS	Destination Prefix-ToS	Prefix-ToS	Prefix-Port
Source prefix			X		X	X
Source prefix mask			X		X	X
Destination prefix				X	X	X
Destination prefix mask				X	X	X
Source app port		X				X
Destination app port		X				X
Input interface	X	X	X		X	X
Output interface	X	X		X	X	X
IP protocol		X				X
Source AS	X		X		X	
Destination AS	X			X	X	
ToS	X	X	X	X	X	X

Field	AS-ToS	Protocol Port-ToS	Source Prefix-ToS	Destination Prefix-ToS	Prefix-ToS	Prefix-Port
First time stamp	X	X	X	X		X
Last time stamp	X	X	X	X		X
Number of flows	X	X	X	X		X
Number of packets	X	X	X	X		X
Number of bytes	X	X	X	X		X

NetFlow AS Aggregation Scheme

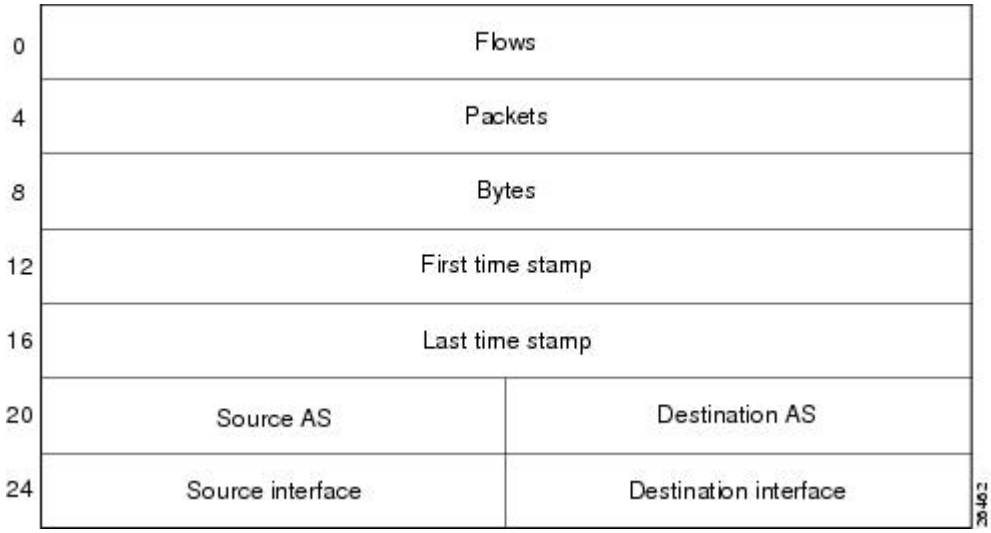
The NetFlow AS aggregation scheme reduces NetFlow export data volume substantially and generates AS-to-AS traffic flow data. The scheme groups data flows that have the same source BGP AS, destination BGP AS, input interface, and output interface.

The aggregated NetFlow data export records report the following:

- Source and destination BGP AS
- Number of packets summarized by the aggregated record
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Source interface
- Destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the AS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 12 Data Export Format for AS Aggregation Scheme



The table below lists definitions for the data export record fields used in the AS aggregation scheme.

Table 16 Data Export Record Field Definitions for AS Aggregation Scheme

Field	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow AS-ToS Aggregation Scheme

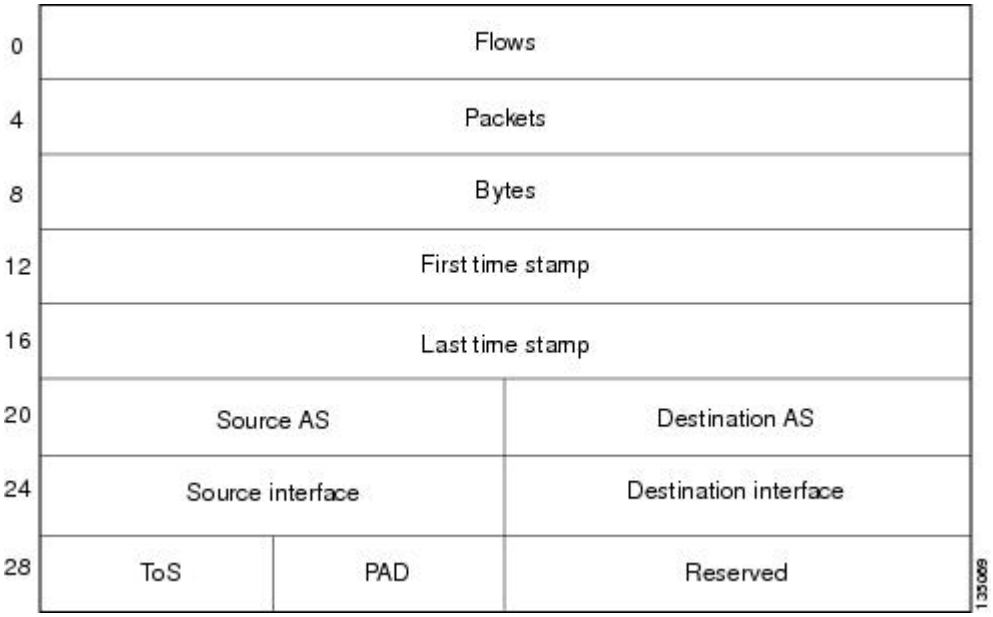
The NetFlow AS-ToS aggregation scheme groups flows that have the same source BGP AS, destination BGP AS, source and destination interfaces, and ToS byte. The aggregated NetFlow export record based on the AS-ToS aggregation scheme reports the following:

- Source BGP AS
- Destination BGP AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by this aggregated record
- Number of packets summarized by this aggregation record
- Source and destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for generating AS-to-AS traffic flow data, and for reducing NetFlow export data volume substantially. The figure below shows the data export format for the AS-ToS

aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 13 Data Export Format for AS-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the AS-ToS aggregation scheme.

Table 17 Data Export Record Term Definitions for AS-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface
ToS	Type of service byte

Term	Definition
PAD	Zero field
Reserved	Zero field

NetFlow Destination Prefix Aggregation Scheme

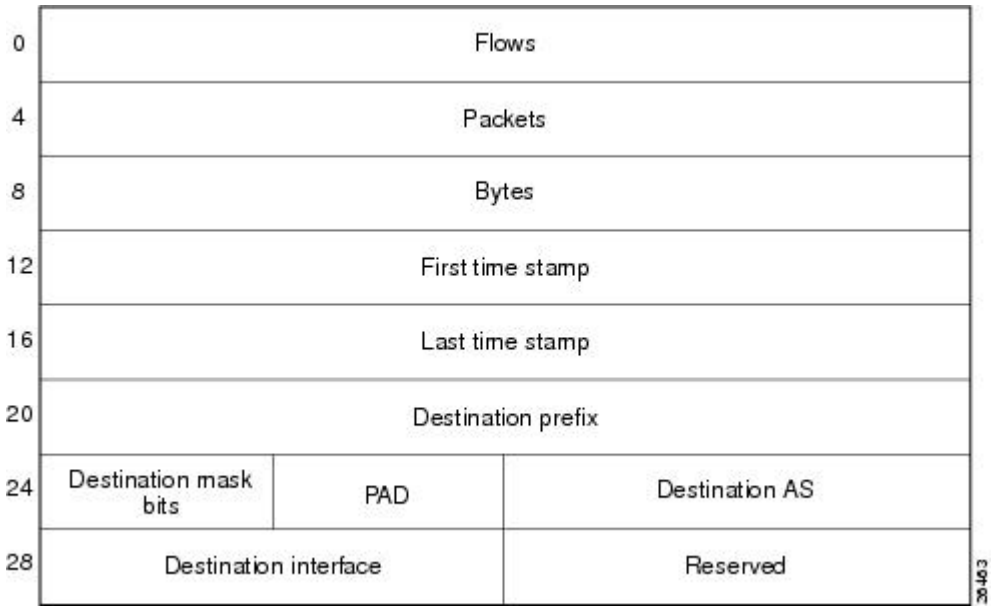
The destination prefix aggregation scheme generates data so that you can examine the destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same destination prefix, destination prefix mask, destination BGP AS, and output interface.

The aggregated NetFlow data export records report the following:

- Destination prefix
- Destination prefix mask
- Destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the destination prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 14 Destination Prefix Aggregation Data Export Record Format



The table below lists definitions for the data export record terms used in the destination prefix aggregation scheme.

Table 18 Data Export Record Term Definitions for Destination Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Destination prefix	Destination IP address ANDed with the destination prefix mask
Destination mask bits	Number of bits in the destination prefix
PAD	Zero field
Destination AS	Autonomous system of the destination IP address (peer or origin)
Destination interface	SNMP index of the output interface
Reserved	Zero field

NetFlow Destination Prefix-ToS Aggregation Scheme

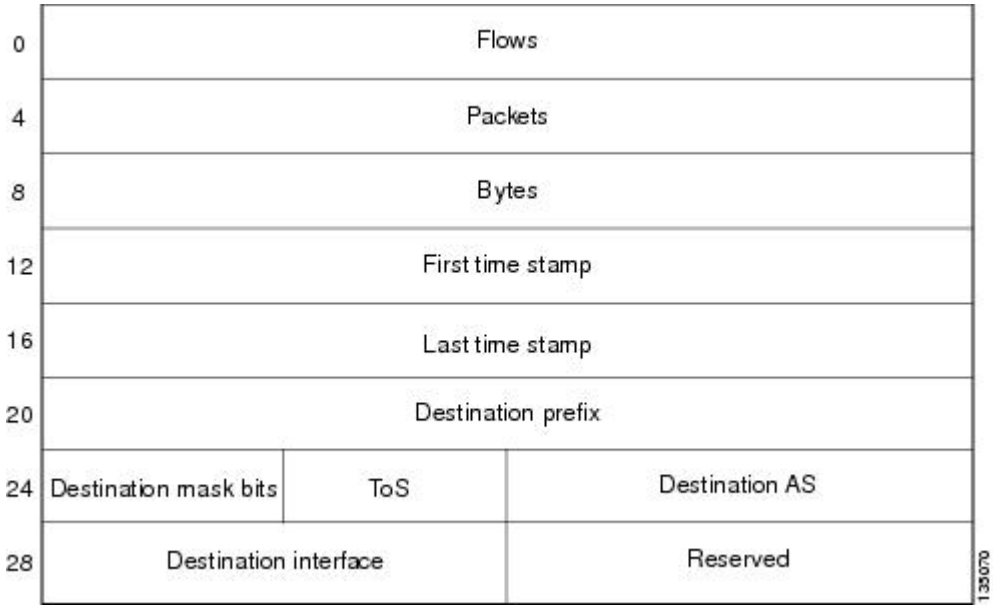
The NetFlow destination prefix-ToS aggregation scheme groups flows that have the same destination prefix, destination prefix mask, destination BGP AS, ToS byte, and output interface. The aggregated NetFlow export record reports the following:

- Destination IP address
- Destination prefix mask
- Destination AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the data

export format for the Destination prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 15 Data Export Format for Destination Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the destination prefix-ToS aggregation scheme.

Table 19 Data Export Record Term Definitions for Destination Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Destination prefix	Destination IP address ANDed with the destination prefix mask
Dest mask bits	Number of bits in the destination prefix
ToS	Type of service byte
Destination AS	Autonomous system of the destination IP address (peer or origin)
Destination interface	SNMP index of the output interface

Term	Definition
Reserved	Zero field

NetFlow Prefix Aggregation Scheme

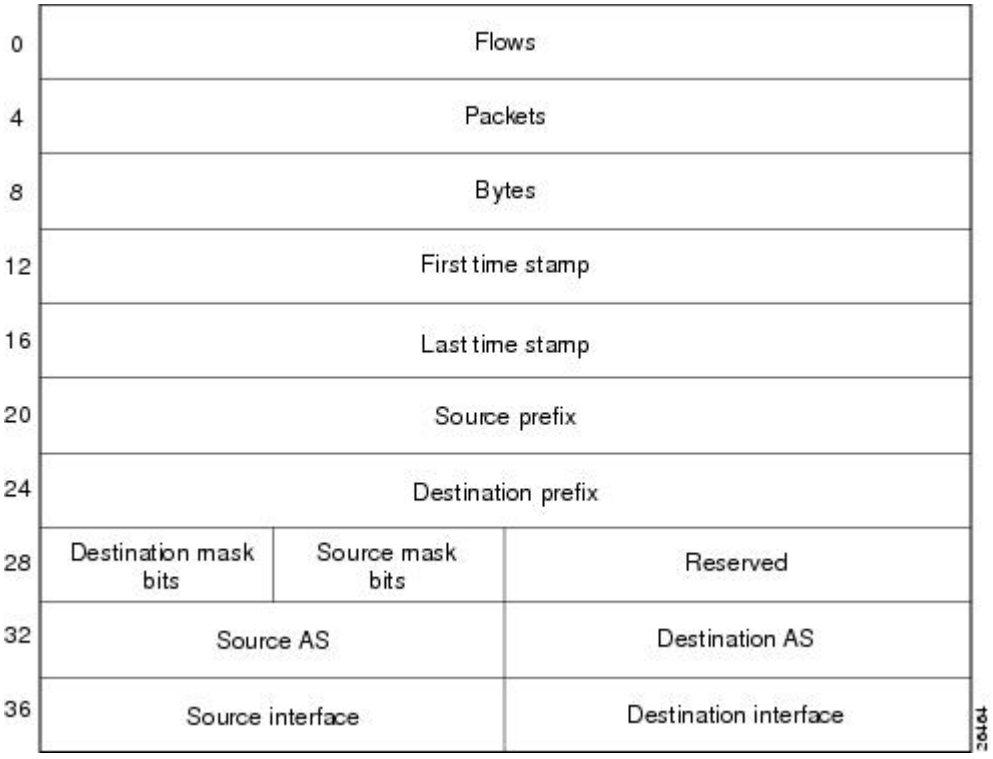
The NetFlow prefix aggregation scheme generates data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, destination prefix, source prefix mask, destination prefix mask, source BGP AS, destination BGP AS, input interface, and output interface.

The aggregated NetFlow data export records report the following:

- Source and destination prefix
- Source and destination prefix mask
- Source and destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input and output interfaces
- Time stamp when the first packet is switched and time stamp when the last packet is switched

The figure below shows the data export format for the prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 16 Data Export Format for Prefix Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix aggregation scheme.

Table 20 Data Export Record Terms and Definitions for Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
Reserved	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Prefix-Port Aggregation Scheme

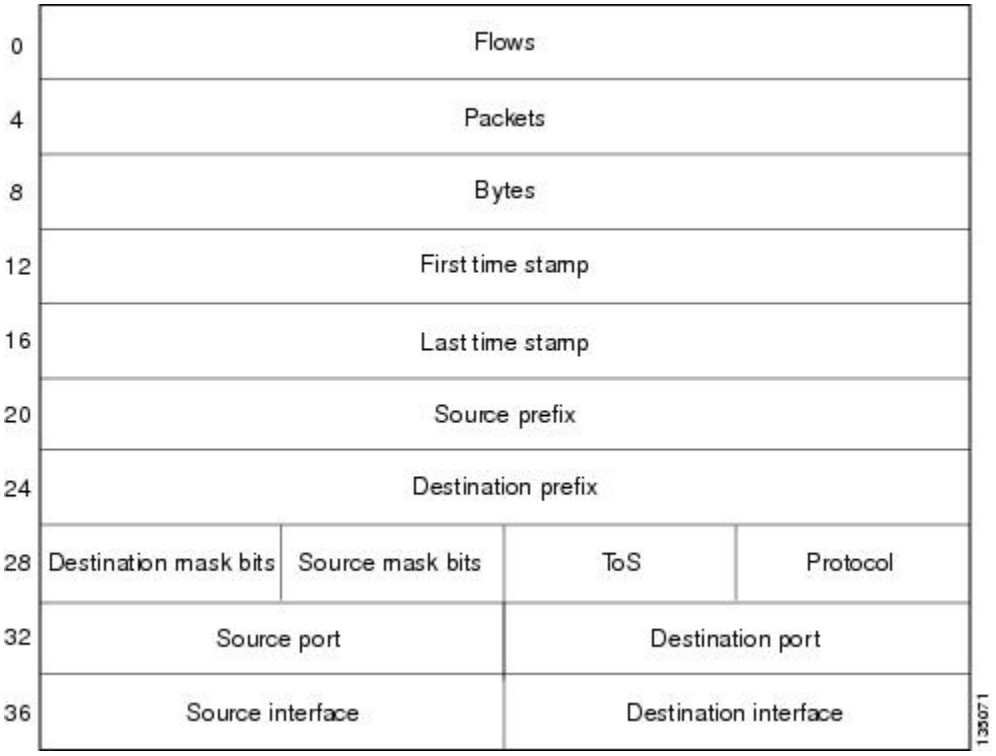
The NetFlow prefix-port aggregation scheme groups flows that have a common source prefix, source mask, destination prefix, destination mask, source port and destination port when applicable, input interface, output interface, protocol, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source port
- Destination port
- Source interface
- Destination interface
- Protocol

- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the data export record for the prefix-port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 17 Data Export Record for Prefix-Port Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix-port aggregation scheme.

Table 21 Data Export Record Term Definitions for Prefix-Port Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched

Term	Definition
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Protocol	IP protocol byte
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Prefix-ToS Aggregation Scheme

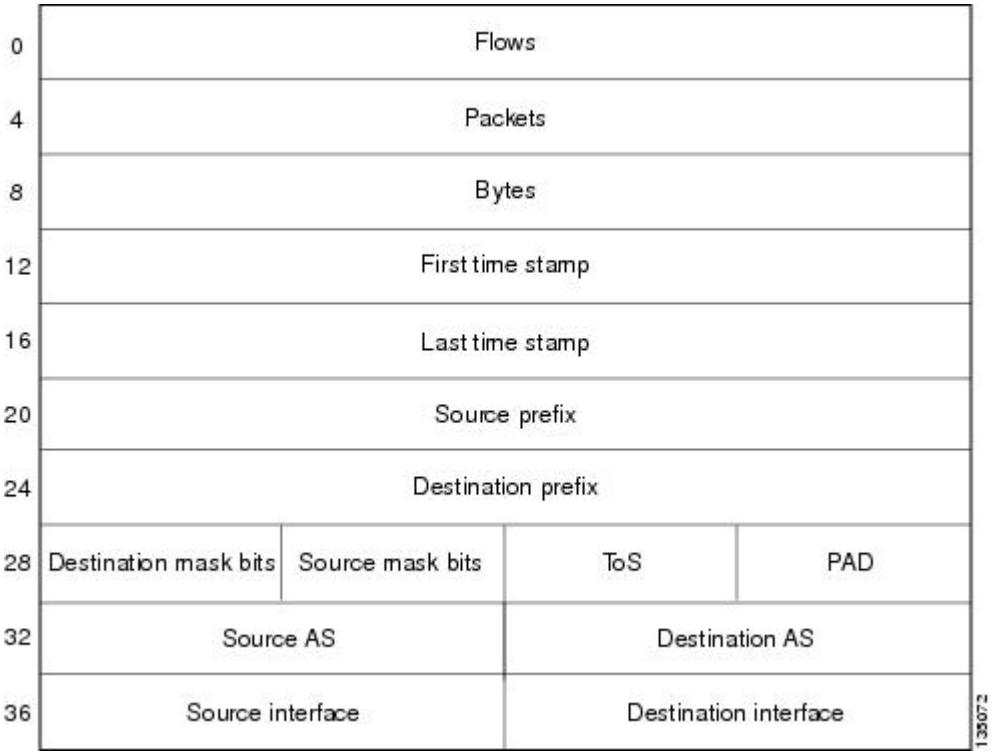
The NetFlow prefix-tos aggregation scheme groups together flows that have a common source prefix, source mask, destination prefix, destination mask, source BGP AS, destination BGP AS, input interface, output interface, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source AS
- Destination AS
- Source interface
- Destination interface
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below displays the

data export format for the prefix-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 18 Data Export Format for Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix-ToS aggregation scheme.

Table 22 Data Export Record Term Definitions for Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Pad	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Protocol Port Aggregation Scheme

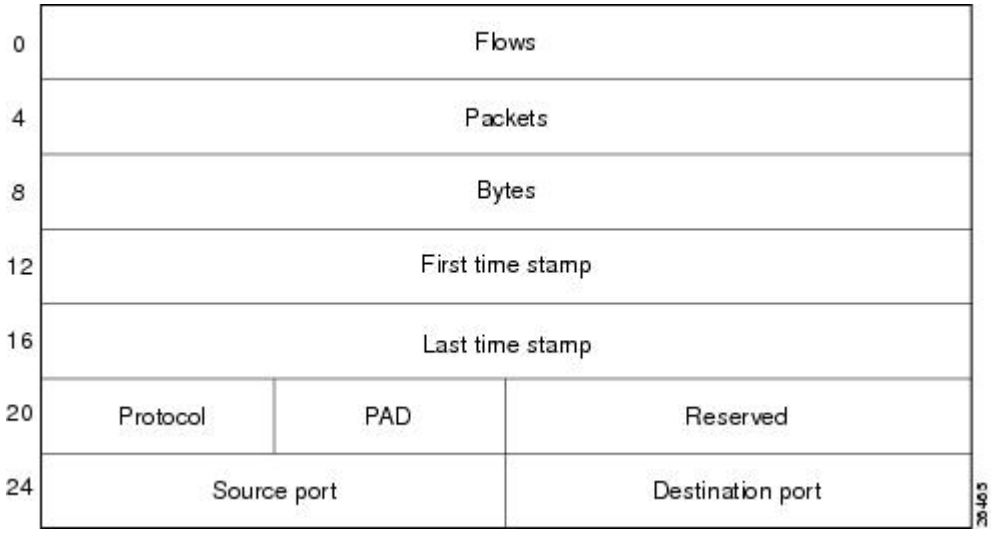
The NetFlow protocol port aggregation scheme captures data so that you can examine network usage by traffic type. The scheme groups data flows with the same IP protocol, source port number, and (when applicable) destination port number.

The aggregated NetFlow data export records report the following:

- Source and destination port numbers
- IP protocol (where 6 = TCP, 17 = UDP, and so on)
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the protocol port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 19 Data Export Format for Protocol Port Aggregation Scheme



The table below lists definitions for the data export record terms used in the protocol port aggregation scheme.

Table 23 Data Export Record Term Definitions for Protocol Port Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Protocol	IP protocol byte
PAD	Zero field
Reserved	Zero field
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number

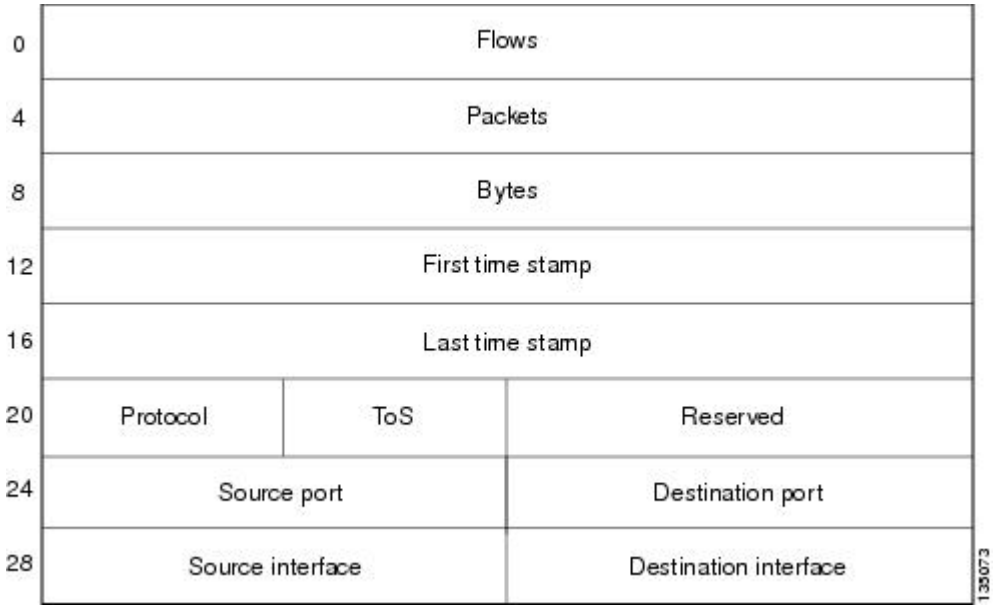
NetFlow Protocol-Port-ToS Aggregation Scheme

The NetFlow protocol-port-tos aggregation scheme groups flows that have a common IP protocol, ToS byte, source and (when applicable) destination port numbers, and source and destination interfaces. The aggregated NetFlow Export record reports the following:

- Source application port number
- Destination port number
- Source and destination interface
- IP protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine network usage by type of traffic. The figure below shows the data export format for the protocol-port-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 20 Data Export Format for Protocol-Port-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the protocol-port-ToS aggregation scheme.

Table 24 Data Export Record Term Definitions for Protocol-Port-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Protocol	IP protocol byte
ToS	Type of service byte
Reserved	Zero field
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number

Term	Definition
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Source Prefix Aggregation Scheme

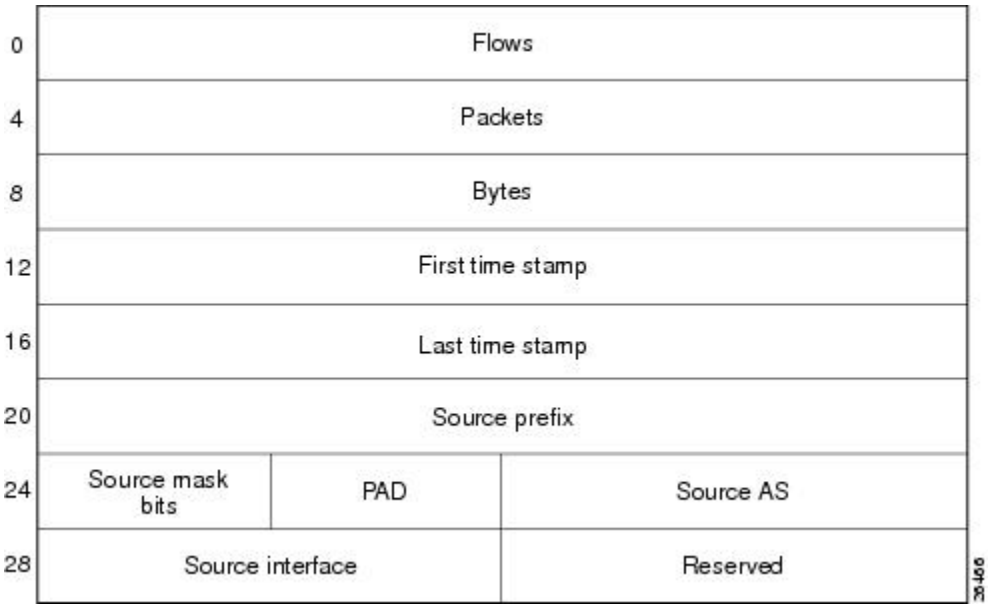
The NetFlow source prefix aggregation scheme captures data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, source prefix mask, source BGP AS, and input interface.

The aggregated NetFlow data export records report the following:

- Source prefix
- Source prefix mask
- Source BGP AS
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below show the data export format for the source prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 21 Data Export Format for Source Prefix Aggregation Scheme



The table below lists definitions for the data export record terms used in the source prefix aggregation scheme.

Table 25 Data Export Record Term Definitions for Source Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Source mask bits	Number of bits in the source prefix
PAD	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Source interface	SNMP index of the input interface
Reserved	Zero field

NetFlow Source Prefix-ToS Aggregation Scheme

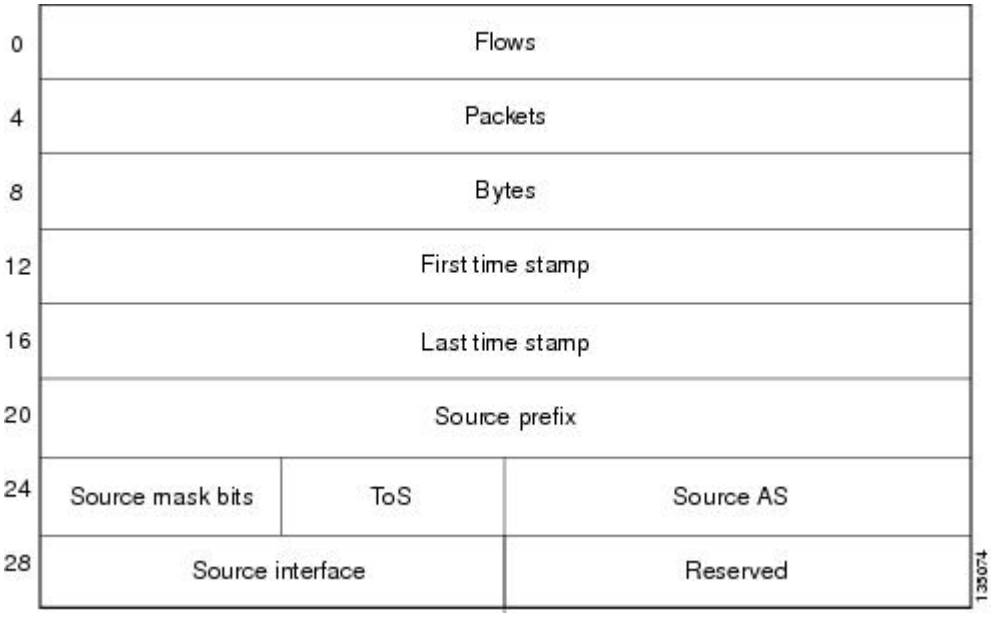
The NetFlow source prefix-ToS aggregation scheme groups flows that have a common source prefix, source prefix mask, source BGP AS, ToS byte, and input interface. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Source AS
- ToS byte
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The figure below show the data export format for the source prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Note When a router does not have a prefix for the source IP address in the flow, NetFlow uses 0.0.0.0 with 0 mask bits rather than making /32 entries. This prevents DOS attacks that use random source addresses from thrashing the aggregation caches. This is also done for the destination in the destination prefix-ToS, the prefix-ToS, and prefix-port aggregation schemes.

Figure 22 Data Export Format for Source Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the source prefix-ToS aggregation scheme.

Table 26 Data Export Record Term Definitions for Source Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Source mask bits	Number of bits in the source prefix

Term	Definition
ToS	Type of service byte
Source AS	Autonomous system of the source IP address (peer or origin)
Source interface	SNMP index of the input interface
Reserved	Zero field

NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview

Export formats available for NetFlow aggregation caches are the Version 9 export format and the Version 8 export format.

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.
- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme. Version 8 is the default export version for aggregation caches when data export is configured.

The Version 9 export format is flexible and extensible, which provides the versatility needed for the support of new fields and record types. You can use the Version 9 export format for both main and aggregation caches.

The Version 8 export format was added to support data export from aggregation caches. This format allows export datagrams to contain a subset of the Version 5 export data that is valid for the cache aggregation scheme.

Refer to the NetFlow Data Export, page 70 section for more details.

How to Configure NetFlow Aggregation Caches

- Configuring NetFlow Aggregation Caches, page 92
- Verifying the Aggregation Cache Configuration, page 96

Configuring NetFlow Aggregation Caches

Perform the steps in this required to enable NetFlow and configure a NetFlow aggregation cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-aggregation cache** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
4. **cache entries** *number*
5. **cache timeout active** *minutes*
6. **cache timeout inactive** *seconds*
7. **export destination** {{*ip-address* | *hostname*} *udp-port*}
8. Repeat Step 7 once to configure a second export destination.
9. **export version** [**9** | **8**]
10. **enabled**
11. **exit**
12. **interface** *interface-type interface-number*
13. **ip flow** {**ingress** | **egress**}
14. **exit**
15. Repeat Steps 12 through 14 to enable NetFlow on other interfaces
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip flow-aggregation cache** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**} **Example:** **Example:** `Router(config)# ip flow-aggregation cache destination-prefix`	(Required) Specifies the aggregation cache scheme and enables aggregation cache configuration mode. • The **as** keyword configures the AS aggregation cache. • The **as-tos**keyword configures the AS ToS aggregation cache. • The **bgp-nexthop-tos** keyword configures the BGP nexthop aggregation cache. • The **destination-prefix** keyword configures the destination prefix aggregation cache. • The **destination-prefix-tos** keyword configures the destination prefix ToS aggregation cache. • The **prefix** keyword configures the prefix aggregation cache. • The **prefix-port** keyword configures the prefix port aggregation cache. • The **prefix-tos** keyword configures the prefix ToS aggregation cache. • The **protocol-port** keyword configures the protocol port aggregation cache. • The **protocol-port-tos** keyword configures the protocol port ToS aggregation cache. • The **source-prefix** keyword configures the source prefix aggregation cache. • The **source-prefix-tos** keyword configures the source prefix ToS aggregation cache.
Step 4	**cache entries** *number* **Example:** `Router(config-flow-cache)# cache entries 2048`	(Optional) Configures aggregation cache operational parameters. • The **entries** *number* keyword-argument pair is the number of cached entries allowed in the aggregation cache. The range is from 1024 to 524288. The default is 4096.
Step 5	**cache timeout active** *minutes* **Example:** `Router(config-flow-cache)# cache timeout active 15`	(Optional) Configures aggregation cache operational parameters. • The **timeout** keyword dissolves the session in the aggregation cache. • The **active** *minutes* keyword-argument pair specifies the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 6	**cache timeout inactive** *seconds* **Example:** `Router(config-flow-cache)# cache timeout inactive 300`	(Optional) Configures aggregation cache operational parameters. • The **timeout** keyword dissolves the session in the aggregation cache. • The **inactive** *seconds*keyword-argument pair specifies the number of seconds that an inactive entry stays in the aggregation cache before the entry times out. The range is from 10 to 600 seconds. The default is 15 seconds.

	Command or Action	Purpose
Step 7	**export destination** {{*ip-address* | *hostname*} *udp-port*} **Example:** `Router(config-flow-cache)# export destination 172.30.0.1 991`	(Optional) Enables the exporting of information from NetFlow aggregation caches. • The *ip-address* | *hostname*argument is the destination IP address or hostname. • The *port* argument is the destination UDP port.
Step 8	Repeat Step 7 once to configure a second export destination.	(Optional) You can configure a maximum of two export destinations for each NetFlow aggregation cache.
Step 9	**export version** [**9** | **8**] **Example:** `Router(config-flow-cache)# export version 9`	(Optional) Specifies data export format Version. • The **version 9** keyword specifies that the export packet uses the Version 9 format.
Step 10	**enabled** **Example:** `Router(config-flow-cache)# enabled`	(Required) Enables the aggregation cache.
Step 11	**exit** **Example:** `Router(config-if)# exit`	(Required) Exits NetFlow aggregation cache configuration mode and returns to global configuration mode.
Step 12	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 13	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --captures traffic that is being received by the interface • **egress** --captures traffic that is being transmitted by the interface.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 15	Repeat Steps 12 through 14 to enable NetFlow on other interfaces	(Optional) --
Step 16	**end** **Example:** `Router(config-if)#` **end**	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Aggregation Cache Configuration

Perform the steps in this optional task to verify that:

- The NetFlow aggregation cache is operational
- NetFlow Data Export for the aggregation cache is operational
- To view the aggregation cache statistics.

SUMMARY STEPS

1. **show ip cache flow aggregation** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
2. **show ip flow export**

DETAILED STEPS

Step 1 **show ip cache flow aggregation** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}

Use the **show ip cache flow aggregation destination-prefix** command to verify the configuration of an destination-prefix aggregation cache. For example:

Example:

```
Router# show ip cache flow aggregation destination-prefix
IP Flow Switching Cache, 139272 bytes
  5 active, 2043 inactive, 9 added
  841 ager polls, 0 flow alloc failures
  Active flows timeout in 15 minutes
  Inactive flows timeout in 300 seconds
IP Sub Flow Cache, 11144 bytes
  5 active, 507 inactive, 9 added, 9 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
```

```
Dst If         Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Null           0.0.0.0         /0   0        5    13    52   138.9
Et0/0.1        172.16.6.0      /24  0        1     1    56     0.0
Et1/0.1        172.16.7.0      /24  0        3    31K 1314   187.3
Et0/0.1        172.16.1.0      /24  0       16   104K 1398   188.4
Et1/0.1        172.16.10.0     /24  0        9    99K 1412   183.3
Router#
```

Use the **show ip cache verbose flow aggregation source-prefix**command to verify the configuration of a source-prefix aggregation cache. For example:

Example:

```
Router# show ip cache verbose flow aggregation source-prefix
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  51 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  4 active, 1020 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Et1/0.1        172.16.10.0     /24  0        4    35K 1391    67.9
Et0/0.1        172.16.6.0      /24  0        2     5    88    60.6
Et1/0.1        172.16.7.0      /24  0        2  3515  1423    58.6
Et0/0.1        172.16.1.0      /24  0        2    20K 1416    71.9
Router#
```

Use the **show ip cache verbose flow aggregation protocol-port** command to verify the configuration of a protocol-port aggregation cache. For example:

Example:

```
Router# show ip cache verbose flow aggregation protocol-port
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  158 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
  0x01       0x0000      0x0000      6       52K     1405        104.3
  0x11       0x0208      0x0208      1        3        52         56.9
  0x01       0x0000      0x0800      2      846      1500         59.8
  0x01       0x0000      0x0B01      2       10        56         63.0
Router#
```

Step 2 **show ip flow export**

Use the **show ip flow export** command to verify that NetFlow Data Export is operational for the aggregation cache. For example:

Example:

```
Router# show ip flow export
Flow export v1 is disabled for main cache
  Version 1 flow records
  Cache for protocol-port aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
```

```
  Cache for source-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for destination-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  40 flows exported in 20 udp datagrams
  0 flows failed due to lack of export packet
  20 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Configuration Examples for Configuring NetFlow Aggregation Caches

- Configuring an AS Aggregation Cache Example, page 98
- Configuring a Destination Prefix Aggregation Cache Example, page 99
- Configuring a Prefix Aggregation Cache Example, page 99
- Configuring a Protocol Port Aggregation Cache Example, page 99
- Configuring a Source Prefix Aggregation Cache Example, page 100
- Configuring an AS-ToS Aggregation Cache Example, page 100
- Configuring a Prefix-ToS Aggregation Cache Example, page 100
- Configuring the Minimum Mask of a Prefix Aggregation Scheme Example, page 101
- Configuring the Minimum Mask of a Destination Prefix Aggregation Scheme Example, page 101
- Configuring the Minimum Mask of a Source Prefix Aggregation Scheme Example, page 101
- Configuring NetFlow Version 9 Data Export for Aggregation Caches Example, page 102
- Configuring NetFlow Version 8 Data Export for Aggregation Caches Example, page 102

Configuring an AS Aggregation Cache Example

The following example shows how to configure an AS aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal
!
ip flow-aggregation cache as
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Destination Prefix Aggregation Cache Example

The following example shows how to configure a destination prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Prefix Aggregation Cache Example

The following example shows how to configure a prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Protocol Port Aggregation Cache Example

The following example shows how to configure a protocol port aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache protocol-port
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
```

```
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Source Prefix Aggregation Cache Example

The following example shows how to configure a source prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring an AS-ToS Aggregation Cache Example

The following example shows how to configure an AS-ToS aggregation cache with a cache active timeout of 20 minutes, an export destination IP address of 10.2.2.2, and a destination port of 9991:

```
configure terminal

!

ip flow-aggregation cache as-tos
 cache timeout active 20
 export destination 10.2.2.2 9991
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Prefix-ToS Aggregation Cache Example

The following example shows how to configure a prefix-ToS aggregation cache with an export destination IP address of 10.4.4.4 and a destination port of 9995:

```
configure terminal

!

ip flow-aggregation cache prefix-tos
 export destination 10.4.4.4 9995
 enabled
!
```

```
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache prefix
 mask source minimum 24
 mask destination minimum 28
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Destination Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a destination prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 mask destination minimum 32
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Source Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a source prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 mask source minimum 30
 enabled
!
interface Ethernet0/0
 ip flow ingress
```

```
!
 end
```

Configuring NetFlow Version 9 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 9 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export template refresh-rate 10
 export version 9
 export template timeout-rate 60
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring NetFlow Version 8 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 8 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export destination 10.42.41.1 9991
 export version 8
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow

Related Topic	Document Title
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBS are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Aggregation Caches

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 27 Feature Information for Configuring NetFlow Aggregation Caches

Feature Name	Releases	Feature Configuration Information
NetFlow ToS-Based Router Aggregation	12.0(15)S 12.2(4)T 12.2(14)S 15.0(1)S	The NetFlow ToS-Based Router Aggregation feature enables you to limit router-based type of service (ToS) aggregation of NetFlow export data. The aggregation of export data provides a summarized NetFlow export data that can be exported to a collection device. The result is lower bandwidth requirements for NetFlow export data and reduced platform requirements for NetFlow data collection devices. The following commands were modified by this feature: **ip flow-aggregation cache**, **show ip cache verbose flow aggregation**, and **show ip flow export**.
NetFlow Minimum Prefix Mask for Router-Based Aggregation	12.0(11)S 12.1(2)T	The NetFlow Minimum Prefix Mask for Router-Based Aggregation feature allows you to set a minimum mask size for prefix aggregation, destination prefix aggregation, and source prefix aggregation schemes. The following commands were modified by this feature: **ip flow-aggregation cache**, **mask destination**, **mask source**, and **show ip cache flow aggregation**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --Distributed Cisco Express Forwarding. Type of CEF switching in which line cards maintain an identical copy of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --Type of packet built by a device (for example, a router) with NetFlow services enabled. The packet contains NetFlow statistics and is addressed to another device (for example, the NetFlow Collection Engine). The other device processes the packet (parses, aggregates, and stores information on IP flows).

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

flowset --Collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two different types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

NetFlow --Cisco IOS accounting feature that maintains per-flow information.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

QoS --quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

template flowset --One or more template records that are grouped in an export packet.

ToS --type of service. The second byte in the IP header. It indicates the desired quality of service (QoS) for a particular datagram.

Configuring NetFlow BGP Next Hop Support for Accounting and Analysis

This document provides information about and instructions for configuring NetFlow Border Gateway Protocol (BGP) next hop support. This feature lets you measure network traffic on a per BGP next hop basis. NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

- Finding Feature Information, page 107
- Prerequisites for NetFlow BGP Next Hop Support, page 107
- Restrictions for NetFlow BGP Next Hop Support, page 108
- Information About NetFlow BGP Next Hop Support, page 108
- How to Configure NetFlow BGP Next Hop Support, page 109
- Configuration Examples for NetFlow BGP Next Hop Support, page 113
- Additional References, page 113
- Feature Information for NetFlow BGP Next Hop Support, page 114
- Glossary, page 115

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for NetFlow BGP Next Hop Support

Before you can configure the NetFlow BGP Next Hop Support feature, you must:

- Configure the router for IP routing
- Configure Cisco Express Forwarding (formerly known as CEF) switching or distributed Cisco Express Forwarding (formerly known as dCEF) switching on the router and on the interfaces that you want to enable NetFlow on (fast switching is not supported)
- Configure NetFlow v9 (Version 9) data export (if only Version 5 is configured, then BGP next hop data is visible in the caches, but is not exported)

- Configure BGP

Restrictions for NetFlow BGP Next Hop Support

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later releases the **ip flow ingress** command is used to enable NetFlow on an interface.

Recursive Load Sharing

The NetFlow cache does not capture the BGP next hop when the route to that BGP next hop is recursively load-shared via several IGP links. Instead, the NetFlow cache captures (as the BGP next hop) the effective simple next hop from among a random selection of the load-shared routes to which the BGP route recurses.

Memory Impact

For BGP-controlled routes, the NetFlow BGP Next Hop Support feature adds 16 bytes to each NetFlow flow record. This increases memory requirements by 16 bytes times the number of flow cache entries that have BGP-controlled prefixes.

Performance Impact

Because the BGP next hop is fetched from the Cisco Express Forwarding path only once per flow, the performance impact of the NetFlow BGP Next Hop Support feature is minimal.

IPv6 and BGP Next Hop

When connected at Layer 3 using an IPv6 address, BGP installs a link-local next hop and a null BGP next hop in Cisco Express Forwarding. NetFlow uses the IPv6 predefined record "netflow ipv6 bgp-nexhop" or a user-defined record containing the match field "routing next-hop address ipv6 bgp" and matches the link-local next hop and a null BGP next hop with the switching software installed on the router.

Information About NetFlow BGP Next Hop Support

- NetFlow BGP Next Hop Support Benefits, page 108
- NetFlow BGP Next Hop Support and NetFlow Aggregation, page 109

NetFlow BGP Next Hop Support Benefits

Without the NetFlow BGP Next Hop Support feature, NetFlow exports only IP next hop information (which provides information for only the next router). This feature adds BGP next hop information to the data export.

The NetFlow BGP Next Hop Support feature lets you find out through which service provider the traffic is going. This functionality is useful if you have arrangements with several other service providers for fault-protected delivery of traffic. The feature lets you charge customers more per packet when traffic has a more

costly destination--you can pass on some of the cost associated with expensive transoceanic links or charge more when traffic is sent to another ISP with which you have an expensive charge agreement.

This feature requires the NetFlow Version 9 export format for its data export.

NetFlow BGP Next Hop Support and NetFlow Aggregation

The Cisco IOS NetFlow Aggregation feature summarizes NetFlow export data on a router before the data is exported to the NetFlow Collection Engine (formerly called the NetFlow FlowCollector). The NetFlow BGP Next Hop Support feature provides the BGP next hop and its related aggregation scheme and provides BGP next hop information within each NetFlow record.

How to Configure NetFlow BGP Next Hop Support

- Configuring NetFlow BGP Next Hop Accounting, page 109
- Verifying the Configuration, page 111

Configuring NetFlow BGP Next Hop Accounting

Perform this task to configure NetFlow BGP next hop accounting for the main cache and aggregation caches. You can enable the export of origin autonomous system (AS) information or peer AS information, but not both.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export version 9** [**origin-as** | **peer-as**] **bgp-nexthop**
4. **ip flow-aggregation cache bgp-nexthop-tos**
5. **enabled**
6. **exit**
7. **interface** *interface-type interface-number*
8. **ip flow** {**ingress** | **egress**}
9. **exit**
10. Repeat Steps 7 through 9 to enable NetFlow on other interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip flow-export version 9** [**origin-as** | **peer-as**] **bgp-nexthop** **Example:** `Router(config)# ip flow-export version 9 origin-as bgp-nexthop`	Enables the export of information in NetFlow cache entries. • **version 9**-- Specifies that the export packet uses the Version 9 format. • **origin-as** --Includes the origin autonomous system (AS) for the source and destination in the export statistics. • **peer-as**-- Includes the peer AS for the source and destination in the export statistics. • **bgp-nexthop** --Includes BGP next hop-related information in the export statistics. This command enables the export of origin AS information and BGP next hop information from the NetFlow main cache. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 4	**ip flow-aggregation cache bgp-nexthop-tos** **Example:** `Router(config)# ip flow-aggregation cache bgp-nexthop-tos`	(Optional) Enables NetFlow aggregation cache schemes and enters aggregation cache configuration mode. • **bgp-nexthop-tos** --Configures the BGP next hop type of service (ToS) aggregation cache scheme.
Step 5	**enabled** **Example:** `Router(config-flow-cache)# enabled`	Enables the aggregation cache.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits aggregation cache configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on an interface.

	Command or Action	Purpose
Step 7	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.
Step 8	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface. • **egress** --Captures traffic that is being transmitted by the interface.
Step 9	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 10	Repeat Steps 7 through 9 to enable NetFlow on other interfaces.	(Optional) --

• Troubleshooting Tips, page 111

Troubleshooting Tips

If there are no BGP-specific flow records in the NetFlow cache, make sure that Cisco Express Forwarding or distributed Cisco Express Forwarding switching is enabled and that the destination for NetFlow data export is configured. Check the routing table for BGP routes also.

Verifying the Configuration

Perform this task to verify the configuration of NetFlow BGP next hop accounting.

SUMMARY STEPS

1. **enable**
2. **show ip cache verbose flow**
3. **show ip cache flow aggregation bgp-nexthop-tos**
4. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if required. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show ip cache verbose flow**

Use this command to verify successful configuration of NetFlow BGP next hop accounting. For example:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (120 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 17826816 bytes
  8 active, 262136 inactive, 8 added
  26 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 1081480 bytes
  8 active, 65528 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk   Active
MUL:M_Opaks  M_Obytes BGP:BGP_NextHop
Et0/0/2        12.0.0.2        Et0/0/4        13.0.0.5        01 00  10   20
0000 /8  0                     0800 /8  0     11.0.0.6              100   0.0
BGP:26.0.0.6
Et0/0/2        12.0.0.2        Et0/0/4        15.0.0.7        01 00  10   20
0000 /8  0                     0800 /8  0     11.0.0.6              100   0.0
BGP:26.0.0.6
Et0/0/2        12.0.0.2        Et0/0/4        15.0.0.7        01 00  10   20
0000 /8  0                     0000 /8  0     11.0.0.6              100   0.0
BGP:26.0.0.6
```

This command displays a detailed summary of NetFlow statistics (including additional NetFlow fields in the header when NetFlow Version 9 data export is configured).

Step 3 **show ip cache flow aggregation bgp-nexthop-tos**

Use this command to verify the configuration of a BGP next hop ToS aggregation cache. For example:

Example:

```
Router# show ip cache flow aggregation bgp-nexthop-tos
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 1 added
  8 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17224 bytes
  1 active, 1023 inactive, 1 added, 1 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src AS  Dst If         Dst AS  TOS Flows   Pkts  B/Pk
Active
BGP NextHop
Et0/0/2        0       Et0/0/4           0     00    9     36     40
8.2
BGP:26.0.0.6
```

Step 4 **exit**

Return to user EXEC mode. For example:

Example:

```
Router# exit
Router>
```

Configuration Examples for NetFlow BGP Next Hop Support

- Example Configuring NetFlow BGP Next Hop Accounting, page 113

Example Configuring NetFlow BGP Next Hop Accounting

The following example shows how to configure NetFlow BGP next hop accounting with origin AS and BGP next hop statistics for the main cache:

```
configure terminal
!
ip flow-export version 9 origin-as bgp-nexthop
ip flow-export destination 172.16.10.2 991
!
interface ethernet 0/0
 ip flow ingress
!
end
```

The following example shows how to configure a NetFlow BGP next hop ToS aggregation cache scheme:

```
configure terminal

!

 ip flow-aggregation cache bgp-nexthop-tos
 export destination 172.16.10.2 991
 enabled
!
interface ethernet 0/0
 ip flow ingress
!
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
NetFlow commands	*Cisco IOS NetFlow Command Reference*
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
Configuring NetFlow and NetFlow Data Export	Configuring NetFlow and NetFlow Data Export

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NetFlow BGP Next Hop Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 28 Feature Information for NetFlow BGP Next Hop Support

Feature Name	Software	Feature Configuration Information
NetFlow BGP Next Hop Support	12.0(26)S 12.2(18)S 12.2(27)SBC 12.3(1) 15.0(1)S	The NetFlow Border Gateway Protocol (BGP) Next Hop Support feature lets you measure network traffic on a per BGP next hop basis. Without the NetFlow BGP Next Hop Support feature, NetFlow exports only IP next hop information (which provides only the address of the next router). This feature adds BGP next hop information to the data export. The following commands were introduced or modified: **ip flow-aggregation cache**, **ip flow-export**, **show ip cache flow aggregation**, **show ip cache verbose flow**.

Glossary

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a specific destination.

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

fast switching --Cisco feature in which a route cache expedites packet switching through a router.

FIB --forwarding information base. A table containing the information needed to forward IP datagrams. At a minimum, this table contains the interface identifier and next hop information for each reachable destination network prefix. The FIB is distinct from the routing table (also called the routing information base), which holds all routing information received from routing peers.

flow --(NetFlow) A set of packets with the same source IP address, destination IP address, source and destination ports, and type of service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine.

This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

ToS --type of service byte. Second byte in the IP header that indicates the desired quality of service for a particular datagram.

Configuring NetFlow BGP Next Hop Support for Accounting and Analysis

This document provides information about and instructions for configuring NetFlow Border Gateway Protocol (BGP) next hop support. This feature lets you measure network traffic on a per BGP next hop basis. NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

- Finding Feature Information, page 117
- Prerequisites for NetFlow BGP Next Hop Support, page 117
- Restrictions for NetFlow BGP Next Hop Support, page 118
- Information About NetFlow BGP Next Hop Support, page 118
- How to Configure NetFlow BGP Next Hop Support, page 119
- Configuration Examples for NetFlow BGP Next Hop Support, page 123
- Additional References, page 123
- Feature Information for NetFlow BGP Next Hop Support, page 124
- Glossary, page 125

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for NetFlow BGP Next Hop Support

Before you can configure the NetFlow BGP Next Hop Support feature, you must:

- Configure the router for IP routing
- Configure Cisco Express Forwarding (formerly known as CEF) switching or distributed Cisco Express Forwarding (formerly known as dCEF) switching on the router and on the interfaces that you want to enable NetFlow on (fast switching is not supported)
- Configure NetFlow v9 (Version 9) data export (if only Version 5 is configured, then BGP next hop data is visible in the caches, but is not exported)

- Configure BGP

Restrictions for NetFlow BGP Next Hop Support

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later releases the **ip flow ingress** command is used to enable NetFlow on an interface.

Recursive Load Sharing

The NetFlow cache does not capture the BGP next hop when the route to that BGP next hop is recursively load-shared via several IGP links. Instead, the NetFlow cache captures (as the BGP next hop) the effective simple next hop from among a random selection of the load-shared routes to which the BGP route recurses.

Memory Impact

For BGP-controlled routes, the NetFlow BGP Next Hop Support feature adds 16 bytes to each NetFlow flow record. This increases memory requirements by 16 bytes times the number of flow cache entries that have BGP-controlled prefixes.

Performance Impact

Because the BGP next hop is fetched from the Cisco Express Forwarding path only once per flow, the performance impact of the NetFlow BGP Next Hop Support feature is minimal.

IPv6 and BGP Next Hop

When connected at Layer 3 using an IPv6 address, BGP installs a link-local next hop and a null BGP next hop in Cisco Express Forwarding. NetFlow uses the IPv6 predefined record "netflow ipv6 bgp-nexhop" or a user-defined record containing the match field "routing next-hop address ipv6 bgp" and matches the link-local next hop and a null BGP next hop with the switching software installed on the router.

Information About NetFlow BGP Next Hop Support

- NetFlow BGP Next Hop Support Benefits, page 108
- NetFlow BGP Next Hop Support and NetFlow Aggregation, page 109

NetFlow BGP Next Hop Support Benefits

Without the NetFlow BGP Next Hop Support feature, NetFlow exports only IP next hop information (which provides information for only the next router). This feature adds BGP next hop information to the data export.

The NetFlow BGP Next Hop Support feature lets you find out through which service provider the traffic is going. This functionality is useful if you have arrangements with several other service providers for fault-protected delivery of traffic. The feature lets you charge customers more per packet when traffic has a more

costly destination--you can pass on some of the cost associated with expensive transoceanic links or charge more when traffic is sent to another ISP with which you have an expensive charge agreement.

This feature requires the NetFlow Version 9 export format for its data export.

NetFlow BGP Next Hop Support and NetFlow Aggregation

The Cisco IOS NetFlow Aggregation feature summarizes NetFlow export data on a router before the data is exported to the NetFlow Collection Engine (formerly called the NetFlow FlowCollector). The NetFlow BGP Next Hop Support feature provides the BGP next hop and its related aggregation scheme and provides BGP next hop information within each NetFlow record.

How to Configure NetFlow BGP Next Hop Support

- Configuring NetFlow BGP Next Hop Accounting, page 109
- Verifying the Configuration, page 111

Configuring NetFlow BGP Next Hop Accounting

Perform this task to configure NetFlow BGP next hop accounting for the main cache and aggregation caches. You can enable the export of origin autonomous system (AS) information or peer AS information, but not both.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export version 9** [**origin-as** | **peer-as**] **bgp-nexthop**
4. **ip flow-aggregation cache bgp-nexthop-tos**
5. **enabled**
6. **exit**
7. **interface** *interface-type interface-number*
8. **ip flow** {**ingress** | **egress**}
9. **exit**
10. Repeat Steps 7 through 9 to enable NetFlow on other interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip flow-export version 9** [**origin-as** | **peer-as**] **bgp-nexthop** **Example:** `Router(config)# ip flow-export version 9 origin-as bgp-nexthop`	Enables the export of information in NetFlow cache entries. • **version 9**-- Specifies that the export packet uses the Version 9 format. • **origin-as** --Includes the origin autonomous system (AS) for the source and destination in the export statistics. • **peer-as**-- Includes the peer AS for the source and destination in the export statistics. • **bgp-nexthop** --Includes BGP next hop-related information in the export statistics. This command enables the export of origin AS information and BGP next hop information from the NetFlow main cache. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 4	**ip flow-aggregation cache bgp-nexthop-tos** **Example:** `Router(config)# ip flow-aggregation cache bgp-nexthop-tos`	(Optional) Enables NetFlow aggregation cache schemes and enters aggregation cache configuration mode. • **bgp-nexthop-tos** --Configures the BGP next hop type of service (ToS) aggregation cache scheme.
Step 5	**enabled** **Example:** `Router(config-flow-cache)# enabled`	Enables the aggregation cache.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits aggregation cache configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on an interface.

	Command or Action	Purpose
Step 7	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.
Step 8	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface. • **egress** --Captures traffic that is being transmitted by the interface.
Step 9	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 10	Repeat Steps 7 through 9 to enable NetFlow on other interfaces.	(Optional) --

• Troubleshooting Tips, page 111

Troubleshooting Tips

If there are no BGP-specific flow records in the NetFlow cache, make sure that Cisco Express Forwarding or distributed Cisco Express Forwarding switching is enabled and that the destination for NetFlow data export is configured. Check the routing table for BGP routes also.

Verifying the Configuration

Perform this task to verify the configuration of NetFlow BGP next hop accounting.

SUMMARY STEPS

1. **enable**
2. **show ip cache verbose flow**
3. **show ip cache flow aggregation bgp-nexthop-tos**
4. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if required. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show ip cache verbose flow**

Use this command to verify successful configuration of NetFlow BGP next hop accounting. For example:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (120 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 17826816 bytes
  8 active, 262136 inactive, 8 added
  26 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 1081480 bytes
  8 active, 65528 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk   Active
MUL:M_Opaks  M_Obytes BGP:BGP_NextHop
Et0/0/2        12.0.0.2        Et0/0/4        13.0.0.5        01 00  10   20
0000 /8  0                     0800 /8  0     11.0.0.6              100   0.0
BGP:26.0.0.6
Et0/0/2        12.0.0.2        Et0/0/4        15.0.0.7        01 00  10   20
0000 /8  0                     0800 /8  0     11.0.0.6              100   0.0
BGP:26.0.0.6
Et0/0/2        12.0.0.2        Et0/0/4        15.0.0.7        01 00  10   20
0000 /8  0                     0000 /8  0     11.0.0.6              100   0.0
BGP:26.0.0.6
```

This command displays a detailed summary of NetFlow statistics (including additional NetFlow fields in the header when NetFlow Version 9 data export is configured).

Step 3 **show ip cache flow aggregation bgp-nexthop-tos**

Use this command to verify the configuration of a BGP next hop ToS aggregation cache. For example:

Example:

```
Router# show ip cache flow aggregation bgp-nexthop-tos
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 1 added
  8 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17224 bytes
  1 active, 1023 inactive, 1 added, 1 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src AS  Dst If         Dst AS  TOS Flows   Pkts  B/Pk
Active
BGP NextHop
Et0/0/2        0       Et0/0/4           0     00    9     36     40
8.2
BGP:26.0.0.6
```

Step 4 **exit**

Return to user EXEC mode. For example:

Example:

```
Router# exit
Router>
```

Configuration Examples for NetFlow BGP Next Hop Support

- Example Configuring NetFlow BGP Next Hop Accounting, page 113

Example Configuring NetFlow BGP Next Hop Accounting

The following example shows how to configure NetFlow BGP next hop accounting with origin AS and BGP next hop statistics for the main cache:

```
configure terminal
!
ip flow-export version 9 origin-as bgp-nexthop
ip flow-export destination 172.16.10.2 991
!
interface ethernet 0/0
 ip flow ingress
!
end
```

The following example shows how to configure a NetFlow BGP next hop ToS aggregation cache scheme:

```
configure terminal

!

 ip flow-aggregation cache bgp-nexthop-tos
 export destination 172.16.10.2 991
 enabled
!
interface ethernet 0/0
 ip flow ingress
!
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
NetFlow commands	*Cisco IOS NetFlow Command Reference*
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
Configuring NetFlow and NetFlow Data Export	Configuring NetFlow and NetFlow Data Export

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NetFlow BGP Next Hop Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 29 Feature Information for NetFlow BGP Next Hop Support

Feature Name	Software	Feature Configuration Information
NetFlow BGP Next Hop Support	12.0(26)S 12.2(18)S 12.2(27)SBC 12.3(1) 15.0(1)S	The NetFlow Border Gateway Protocol (BGP) Next Hop Support feature lets you measure network traffic on a per BGP next hop basis. Without the NetFlow BGP Next Hop Support feature, NetFlow exports only IP next hop information (which provides only the address of the next router). This feature adds BGP next hop information to the data export. The following commands were introduced or modified: **ip flow-aggregation cache**, **ip flow-export**, **show ip cache flow aggregation**, **show ip cache verbose flow**.

Glossary

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a specific destination.

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

fast switching --Cisco feature in which a route cache expedites packet switching through a router.

FIB --forwarding information base. A table containing the information needed to forward IP datagrams. At a minimum, this table contains the interface identifier and next hop information for each reachable destination network prefix. The FIB is distinct from the routing table (also called the routing information base), which holds all routing information received from routing peers.

flow --(NetFlow) A set of packets with the same source IP address, destination IP address, source and destination ports, and type of service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine.

This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

ToS --type of service byte. Second byte in the IP header that indicates the desired quality of service for a particular datagram.

Configuring NetFlow Multicast Accounting

This document contains information about and instructions for configuring NetFlow multicast accounting. NetFlow multicast accounting allows you to capture multicast-specific data (both packets and bytes) for multicast flows.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

- Finding Feature Information, page 127
- Prerequisites for Configuring NetFlow Multicast Accounting, page 127
- Restrictions for Configuring NetFlow Multicast Accounting, page 128
- Information About Configuring NetFlow Multicast Accounting, page 128
- How to Configure NetFlow Multicast Accounting, page 129
- Configuration Examples for NetFlow Multicast Accounting, page 135
- Additional References, page 136
- Feature Information for Configuring NetFlow Multicast Accounting, page 138
- Glossary, page 139

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring NetFlow Multicast Accounting

Before you can configure NetFlow multicast accounting, you must:

- Configure the router for IP routing
- Configure Multicast fast switching or multicast distributed fast switching (MDFS); multicast Cisco Express Forwarding (CEF) switching is not supported.
- Configure Multicast routing.
- Configure NetFlow v9 (Version 9) data export (otherwise, multicast data is visible in the cache but is not exported).

Restrictions for Configuring NetFlow Multicast Accounting

Memory Impact

If traffic is heavy, the additional flows might fill the global flow hash table. If you must increase the size of the global flow hash table, you must also add memory to the router.

NetFlow has a maximum cache size of 65,536 flow record entries of 64 bytes each. To deduce the packet-replication factor, multicast accounting adds 16 bytes (for a total of 80 bytes) to each multicast flow record.

Performance Impact

Ingress multicast accounting does not greatly affect performance. Because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router, egress NetFlow multicast accounting might degrade network performance slightly, but it does not limit the functionality of the router.

Multicast Addresses

NetFlow data cannot be exported to multicast addresses.

Information About Configuring NetFlow Multicast Accounting

- NetFlow Multicast Benefits, page 128
- Multicast Ingress and Multicast Egress Accounting, page 128
- NetFlow Multicast Flow Records, page 129

NetFlow Multicast Benefits

NetFlow multicast allows you to capture multicast-specific data (both packets and bytes) for multicast flows. For example, you can capture the packet-replication factor for a specific flow as well as for each outgoing stream. NetFlow multicast provides complete end-to-end usage information about network traffic for a complete multicast traffic billing solution.

You can use NetFlow multicast accounting to identify and count multicast packets on the ingress side or the egress side (or both sides) of a router. Multicast ingress accounting provides information about the source and how many times the traffic was replicated. Multicast egress accounting monitors the destination of the traffic flow.

NetFlow multicast lets you enable NetFlow statistics to account for all packets that fail the reverse path forwarding (RPF) check and that are dropped in the core of the service provider network. Accounting for RPF-failed packets provides more accurate traffic statistics and patterns.

Multicast Ingress and Multicast Egress Accounting

NetFlow multicast lets you select either multicast ingress accounting, in which a replication factor (equal to the number of output interfaces) indicates the load, or multicast egress accounting, in which all outgoing multicast streams are counted as separate streams, or both multicast ingress and multicast egress accounting.

NetFlow multicast lets you collect information about how much data is leaving the interfaces of the router (egress and multicast ingress accounting) or how much multicast data is received (multicast ingress accounting).

On the ingress side, multicast packets are counted as with unicast packets, but with two additional fields (for number of replicated packets and byte count). With multicast ingress accounting, the destination interface field is set to null, and the IP next hop field is set to 0 for multicast flows.

NetFlow Multicast Flow Records

Multicast ingress accounting creates one flow record that indicates how many times each packet is replicated. Multicast egress accounting creates a unique flow record for each outgoing interface.

How to Configure NetFlow Multicast Accounting

- Configuring NetFlow Multicast Accounting in Releases 12.4(12), page 129
- Configuring NetFlow Multicast Accounting in Cisco IOS Releases Prior to 12.4(12), page 131
- Verifying the NetFlow Multicast Accounting Configuration, page 134

Configuring NetFlow Multicast Accounting in Releases 12.4(12)

Perform the steps in this required task to configure NetFlow multicast accounting.

You must have already configured IP multicast on the networking devices in your network. See the *Cisco IOS IP Multicast Configuration Guide* , for more information on configuring IP multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast netflow rpf-failure**
5. **ip multicast netflow output-counters**
6. **interface** *type number*
7. **ip flow ingress**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • The **vrf** keyword supports the multicast Virtual Private Network (VPN) routing/forwarding instance (VRF). • The *vrf-name* argument is the name assigned to the VRF. • The **distributed** keyword enables Multicast Distributed Switching (MDS).
Step 4	**ip multicast netflow rpf-failure** **Example:** `Router(config)# ip multicast netflow rpf-failure`	Enables accounting for multicast data that fails the RPF check.
Step 5	**ip multicast netflow output-counters** **Example:** `Router(config)# ip multicast netflow output-counters`	Enables accounting for the number of bytes and packets forwarded.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies the interface and enters interface configuration mode.
Step 7	**ip flow ingress** **Example:** `Router(config-if)# ip flow ingress`	Enables NetFlow ingress accounting.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 131

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Configuring NetFlow Multicast Accounting in Cisco IOS Releases Prior to 12.4(12)

- Configuring NetFlow Multicast Egress Accounting, page 131
- Configuring NetFlow Multicast Ingress Accounting, page 132

Configuring NetFlow Multicast Egress Accounting

Perform the steps in this required task to configure NetFlow multicast egress accounting.

You must have already configured IP multicast on the networking devices in your network. See the *Cisco IOS IP Multicast Configuration Guide*, for more information on configuring IP multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast netflow rpf-failure**
5. **interface** *type number*
6. **ip multicast netflow egress**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing` **Example:**	Enables IP multicast routing. • The **vrf** keyword supports the multicast Virtual Private Network (VPN) routing/forwarding instance (VRF). • The *vrf-name* argument is the name assigned to the VRF. • The **distributed** keyword enables Multicast Distributed Switching (MDS).
Step 4 **ip multicast netflow rpf-failure** **Example:** `Router(config)# ip multicast netflow rpf-failure`	Enables accounting for multicast data that fails the RPF check.
Step 5 **interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies the interface and enters interface configuration mode.
Step 6 **ip multicast netflow egress** **Example:** `Router(config-if)# ip multicast netflow egress`	Enables NetFlow multicast egress accounting.
Step 7 **end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 132

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Configuring NetFlow Multicast Ingress Accounting

Perform the steps in this required task to configure NetFlow multicast ingress accounting.

Multicast ingress NetFlow accounting is enabled by default.

You must have already configured IP multicast on the networking devices in your network. See the *Cisco IOS IP Multicast Configuration Guide*, for more information on configuring IP multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast netflow rpf-failure**
5. **interface** *type number*
6. **ip multicast netflow ingress**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing` **Example:**	Enables IP multicast routing. • The **vrf** keyword supports the multicast VRF. • The *vrf-name* argument is the name assigned to the VRF. • The **distributed** keyword enables Multicast Distributed Switching (MDS).
Step 4	**ip multicast netflow rpf-failure** **Example:** `Router(config)# ip multicast netflow rpf-failure`	Enables accounting for multicast data that fails the RPF check.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies the interface and enters interface configuration mode.
Step 6	**ip multicast netflow ingress** **Example:** `Router(config-if)# ip multicast netflow ingress`	Enables NetFlow multicast ingress accounting.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 134

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Verifying the NetFlow Multicast Accounting Configuration

Perform the steps in this optional task to verify the NetFlow multicast accounting configuration.

SUMMARY STEPS

1. **enable**
2. **show ip cache verbose flow**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if required. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show ip cache verbose flow**

Use this command to verify that NetFlow multicast accounting is configured. Look for the two additional fields related to multicast data, that is, the number of IP multicast output packet and byte counts. For example:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (5149 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .997 .002 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 14 added
  468 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  1 active, 1023 inactive, 1 added, 1 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other           12      0.0         1    52      0.0       0.1      15.6
Total:              12      0.0         1    52      0.0       0.1      15.6
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
IPM: OPkts    OBytes
Et0/0          10.1.1.1        Null           224.192.16.1    01 55  10    5164
0000 /0  0                     0000 /0  0     0.0.0.0                20   262.8
IPM:    15K    309K
Et0/0          10.1.1.1        Null           255.255.255.255 11 C0  10       1
0208 /0  0                     0208 /0  0     0.0.0.0                52     0.0
Router#
```

The Opkts column displays the number of IP multicast (IPM) output packets, the OBytes column displays the number of IPM output bytes, and the DstIPaddress column displays the destination IP address for the IPM output packets.

Configuration Examples for NetFlow Multicast Accounting

- Configuring NetFlow Multicast Accounting in Original Releases, page 135
- Configuring NetFlow MC Accounting in Releases Prior to 12.2(33)SRB, page 136

Configuring NetFlow Multicast Accounting in Original Releases

The following example shows how to configure multicast NetFlow accounting:

```
configure terminal
 ip multicast-routing
 ip multicast netflow rpf-failure
 ip multicast netflow output-counters
!
interface ethernet 0/0
 ip flow ingress
 end
```

Configuring NetFlow MC Accounting in Releases Prior to 12.2(33)SRB

- Configuring NetFlow Multicast Egress Accounting Example, page 136
- Configuring NetFlow Multicast Ingress Accounting Example, page 136

Configuring NetFlow Multicast Egress Accounting Example

The following example shows how to configure multicast egress NetFlow accounting on the egress Ethernet 0/0 interface:

```
configure terminal
 ip multicast-routing
 ip multicast netflow rpf-failure
!
interface ethernet 0/0
 ip multicast netflow egress
 end
```

Configuring NetFlow Multicast Ingress Accounting Example

The following example shows how to configure multicast ingress NetFlow accounting on the ingress Ethernet 1/0 interface:

```
configure terminal
 ip multicast-routing
 ip multicast netflow rpf-failure
!
interface ethernet 1/0
 ip multicast netflow ingress
 end
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis

Related Topic	Document Title
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBS are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Multicast Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 30 Feature Information for Configuring NetFlow Multicast Accounting

Feature Name	Releases	Feature Configuration Information
NetFlow Multicast Support	12.3(1), 12.2(18)S, 12.2(27)SBC, 12.2(33)SXF, 12.2(33)SRB	The NetFlow Multicast Support feature lets you capture multicast-specific data (both packets and bytes) for multicast flows. For example, you can capture the packet-replication factor for a specific flow as well as for each outgoing stream. This feature provides complete end-to-end usage information about network traffic for a complete multicast traffic billing solution. The following commands were introduced by this feature: **ip multicast netflow egress**, **ip multicast netflow ingress**, and **ip multicast netflow rpf-failure**.
NetFlow Multicast Support[3]	12.4(11)T, 12.4(12), 12.(33)SRB, 12.2(33)SB, 12.2(33)SXH	The **ip multicast netflow** [**ingress** | **egress**] interface configuration command was replaced by the **ip multicast netflow output-counters** global configuration command.

Glossary

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

egress traffic --Traffic leaving the network.

fast switching --Cisco feature in which a route cache is used for expediting packet switching through a router.

ingress traffic --Traffic entering the network.

multicast data --Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address field.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

3 This was a minor modification to the existing NetFlow Multicast Support feature. Minor feature modifications are not included in Feature Navigator.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly called NetFlow FlowCollector)--A Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

RPF --Reverse Path Forwarding. Multicasting technique in which a multicast datagram is forwarded out of all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram.

ToS byte --type of service byte. Second byte in the IP header that indicates the desired quality of service (QoS) for a particular datagram.

Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands

This module contains information about and instructions for configuring NetFlow Top Talkers feature. The NetFlow Top Talkers feature can be configured using the Cisco IOS command-line interface (CLI) or with SNMP commands using the NetFlow MIB. The NetFlow Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. The NetFlow MIB allows you to configure NetFlow and the NetFlow Top Talkers feature using SNMP commands from a network management workstation.

- Finding Feature Information, page 141
- Prerequisites for Configuring NetFlow Top Talkers, page 141
- Restrictions for Configuring NetFlow Top Talkers, page 142
- Information About Configuring NetFlow Top Talkers, page 142
- How to Configure NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands, page 143
- Configuration Examples for NetFlow Top Talkers, page 163
- Additional References, page 164
- Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands, page 166

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring NetFlow Top Talkers

Before you enable NetFlow and NetFlow Top Talkers, you must:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching

- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources.

Restrictions for Configuring NetFlow Top Talkers

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface.

Cisco IOS Release 12.2(33)SXH

Some of the keywords and arguments for the commands used to configure the NetFlow MIB and Top Talkers feature are not supported in 12.2(33)SXH. See the syntax descriptions for the commands in the command reference (URL for the 12.2SX NF CR to be added later) for details.

Information About Configuring NetFlow Top Talkers

- Overview of the NetFlow MIB and Top Talkers Feature, page 142
- Benefits of the NetFlow MIB and Top Talkers Feature, page 143
- Cisco IOS Release 12.2(33)SXH on Cisco 6500 Series Switches, page 143

Overview of the NetFlow MIB and Top Talkers Feature

NetFlow collects traffic flow statistics on routing devices. NetFlow has been used for a variety of applications, including traffic engineering, usage-based billing, and monitoring for denial-of-service (DoS) attacks.

The flows that are generating the heaviest system traffic are known as the "top talkers."

The NetFlow Top Talkers feature allows flows to be sorted so that they can be viewed. The top talkers can be sorted by either of the following criteria:

- By the total number of packets in each top talker
- By the total number of bytes in each top talker

The usual implementation of NetFlow exports NetFlow data to a collector. The NetFlow MIB and Top Talkers feature performs security monitoring and accounting for top talkers and matches and identifies key users of the network. This feature is also useful for a network location where a traditional NetFlow export operation is not possible. The NetFlow MIB and Top Talkers feature does not require a collector to obtain information regarding flows. Instead, these flows are placed in a special cache where they can be viewed. The NetFlow MIB part of the NetFlow MIB and Top Talkers feature allows you to configure the NetFlow Top Talkers feature using SNMP.

In addition to sorting top talkers, you can further organize your output by specifying criteria that the top talkers must match, such as source or destination IP address or port. The **match** command is used to specify this criterion. For a full list of the matching criteria that you can select, refer to the **match**command in the Cisco IOS command reference documentation.

Benefits of the NetFlow MIB and Top Talkers Feature

Top talkers can be useful for analyzing network traffic in any of the following ways:

- Security--You can view the list of top talkers to see if traffic patterns consistent with DoS attack are present in your network.
- Load balancing--You can identify the most heavily used parts of the system and move network traffic over to less-used parts of the system.
- Traffic analysis--Consulting the data retrieved from the NetFlow MIB and Top Talkers feature can assist you in general traffic study and planning for your network.

An additional benefit of the NetFlow MIB and Top Talkers feature is that it can be configured for a router either by entering CLI commands or by entering SNMP commands on a network management system (NMS) workstation. The SNMP commands are sent to the router and processed by a MIB. You do not have to be connected to the router console to extract the list of top talkers information if an NMS workstation is configured to communicate using SNMP to your network device. For more information on configuring your network device to use MIB functionality for the NetFlow MIB and Top Talkers feature, see Configuring SNMP Support on the Networking Device, page 144.

Cisco IOS Release 12.2(33)SXH on Cisco 6500 Series Switches

The **show ip flow top-talkers** command was modified in Cisco IOS Release 12.2(33)SXH for the Cisco 6500 Series switches to support displaying the top talkers for a specific module. The **show ip flow top-talkers module** *number* command displays the top talkers for that module. The **show ip flow top-talkers** command without the module keyword shows the top talkers in the hardware switched path (a merged list of top lists from all modules) and then software switched top talkers. The NetFlow MIB can be used to request the top talker list and to set and/or get the configuration parameters for the NetFlow MIB Top Talkers feature.

How to Configure NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands

Note Some of the tasks in this section include examples of the SNMP CLI syntax used to set configuration parameters on the router and to read values from MIB objects on the router. These SNMP CLI syntax examples are taken from a Linux workstation using public-domain SNMP tools. The SNMP CLI syntax for your workstation might be different. Refer to the documentation that was provided with your SNMP tools for the correct syntax for your network management workstation.

- Configuring SNMP Support on the Networking Device, page 144
- Configuring Parameters for the NetFlow Main Cache, page 145
- Configuring Parameters for the NetFlow Main Cache, page 147
- Identifying the Interface Number to Use for Enabling NetFlow with SNMP, page 147
- Configuring NetFlow on a Cisco 6500 Series Switch, page 148
- Configuring NetFlow on a Cisco 6500 Series Switch, page 150
- Configuring NetFlow on Cisco Routers, page 151
- Configuring NetFlow on Cisco Routers, page 153

- Configuring NetFlow Top Talkers, page 153
- Configuring NetFlow Top Talkers, page 155
- Configuring NetFlow Top Talkers Match Criteria, page 156
- Verifying the NetFlow Top Talkers Configuration, page 161
- Verifying the NetFlow Top Talkers Configuration, page 162

Configuring SNMP Support on the Networking Device

If you want to configure the NetFlow Top Talkers feature using the Cisco IOS CLI, you do not have to perform this task.

If you want to configure the NetFlow Top Talkers feature using the NetFlow MIB and SNMP, you must perform this task.

Before you can use SNMP commands to configure the Top Talkers feature you must configure SNMP support on your networking device. To enable SNMP support on the networking device perform the steps in this task.

Note The SNMP community read-only (RO) string for the examples is **public**. The SNMP community read-write (RW) string for the examples is **private**. You should use more complex strings for these values in your configurations.

Note For more information on configuring SNMP support on your networking device, refer to the "Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide* .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* **ro**
4. **snmp-server community** *string* **rw**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**snmp-server community** *string* **ro** **Example:** `Router(config)# snmp-server community public ro`	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **ro** keyword specifies read-only access. SNMP management stations using this string can retrieve MIB objects.
Step 4	**snmp-server community** *string* **rw** **Example:** `Router(config)# snmp-server community private rw`	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **rw** keyword specifies read-write access. SNMP management stations using this string can retrieve and modify MIB objects. **Note** The *string* argument must be different from the read-only *string* argument specified in the preceding step (Step 3).
Step 5	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Parameters for the NetFlow Main Cache

This optional task describes the procedure for modifying the parameters for the NetFlow main cache. Perform the steps in this optional task using either the router CLI commands or the SNMP commands to modify the parameters for the NetFlow main cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-cache entries** *number*
4. **ip flow-cache timeout active** *minutes*
5. **ip flow-cache timeout inactive** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 4000`	(Optional) Specifies the maximum number of entries to be captured for the main flow cache. • The range for the *number* argument is from 1024 to 524288 entries.
Step 4	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 30`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the cache. • The **active** *minutes* keyword-argument pair is the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 5	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 100`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the main cache. • The **inactive** *seconds*keyword-argument pair is the number of seconds that an inactive entry will stay in the main cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.
Step 6	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Parameters for the NetFlow Main Cache

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.type unsigned** *number*
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.type unsigned** *number*
3. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] c**nfCIInactiveTimeOut.type unsigned** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCICacheEntries.0 unsigned 4000`	(Optional) Defines the maximum number of entries to be captured for the main flow cache. • The value for the *type* argument in **cnfCICacheEntries**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCICacheEntries**.*type number* is the maximum number of cache entries. • The range for the *number* argument is from 1024 to 524288 entries.
Step 2	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIActiveTimeOut.0 unsigned 60`	(Optional) Specifies the number of seconds that an active flow remains in the main cache before it times out. • The value for the *type* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is the number of seconds that an active flow remains in the cache before it times out. • The range for the *number* argument is from 1 to 60 minutes. The default is 30 minutes.
Step 3	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] c**nfCIInactiveTimeOut.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIInactiveTimeOut.0 unsigned 30`	(Optional) Specifies the number of seconds that an inactive flow remains in the main cache before it times out. • The value for the *type* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is the number of seconds that an inactive flow remains in the main cache before it times out. • The range for the *number* argument is from 10 to 600 seconds. The default is 15 seconds.

Identifying the Interface Number to Use for Enabling NetFlow with SNMP

If you want to configure the NetFlow Top Talkers feature using the Cisco IOS CLI, you do not have to perform this task.

If you want to configure the NetFlow Top Talkers feature using the NetFlow MIB and SNMP, you must perform this task.

Before you can use SNMP to enable NetFlow on an interface, you must identify the SNMP interface number on the router. To identify the interface number for the interface on which you want to enable NetFlow, perform the steps in this required task.

SUMMARY STEPS

1. **enable**
2. **show snmp mib ifmib ifindex** *type number*
3. Repeat Step 2 to identify the SNMP interface number for any other interfaces on which you plan to enable NetFlow.

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode. Enter the password if prompted.

Example:

```
Router> enable
```

Step 2 **show snmp mib ifmib ifindex** *type number*
Displays the SNMP interface number for the interface specified.

Example:

```
Router# show snmp mib ifmib ifindex GigabitEthernet6/2
Ethernet0/0: Ifindex = 60
```

Step 3 Repeat Step 2 to identify the SNMP interface number for any other interfaces on which you plan to enable NetFlow.

Configuring NetFlow on a Cisco 6500 Series Switch

To enable NetFlow on the switch, perform the steps in this required task using either the CLI commands or the SNMP commands.

Note This task provides the minimum information required to configure NetFlow on your Cisco 6500 series switch. See the Catalyst 6500 Series Cisco IOS Software Configuration Guide, for more information of configuring NetFlow on your switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}
4. **interface** *type number*
5. **ip flow** {**ingress** | **egress**}
6. **exit**
7. Repeat Steps 4 through 6 to enable NetFlow on other interfaces.
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**mls flow** {**ip**	**ipv6**} {**destination**	**destination-source**	**full**	**interface-destination-source**	**interface-full**	**source**} **Example:** `Router(config)# mls flow ip interface-full`	Specifies the NetFlow flow mask for IPv4 traffic.
Step 4	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet6/2`	(Required) Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.

	Command or Action	Purpose

Step 5	**ip flow** {**ingress** | **egress**}
	
	Example:
	`Router(config-if)# ip flow ingress`
	
	Example:
	
	Example:
	`and/or`
	
	Example:
	`Router(config-if)# ip flow egress`
		(Required) Enables NetFlow on the interface.
		• **ingress** --Captures traffic that is being received by the interface
		• **egress** --Captures traffic that is being transmitted by the interface.

Step 6	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. • Use this command only if you want to enable NetFlow on another interface.
Step 7	Repeat Steps 4 through 6 to enable NetFlow on other interfaces.	(Optional) --
Step 8	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on a Cisco 6500 Series Switch

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cseFlowIPFlowMask integer** [**1** | **2** | **3** | **4** | **5** | **6**]
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCINetflowEnable**.*interface-number* **integer** [**0** | **1** | **2** | **3**]
3. Repeat Step 2 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cseFlowIPFlowMask integer** [**1** | **2** | **3** | **4** | **5** | **6**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1`	Specifies the NetFlow flow mask for IPv4 traffic. • 1--destination-only • 2--source-destination • 3--full-flow • 4--source-only • 5--interface-source-destination • 6--interface-full
Step 2	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCINetflowEnable**.*interface-number* **integer** [**0** | **1** | **2** | **3**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1`	(Required) Configures NetFlow for an interface. • The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode. • The values for the *direction* argument are: ◦ 0--Disable NetFlow ◦ 1--Enable Ingress NetFlow ◦ 2--Enable Egress NetFlow ◦ 3--Enable Ingress and Egress NetFlow
Step 3	Repeat Step 2 to enable NetFlow on other interfaces	(Optional) --

Configuring NetFlow on Cisco Routers

To enable NetFlow on the router, perform the steps in this required task using either the CLI commands or the SNMP commands .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces.
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet6/2`	(Required) Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.

Step 4	**ip flow** {**ingress** | **egress**}
	
	Example:
	`Router(config-if)# ip flow ingress`
	
	Example:
	
	Example:
	`and/or`
	
	Example:
	`Router(config-if)# ip flow egress`
		(Required) Enables NetFlow on the interface.
		• **ingress** --Captures traffic that is being received by the interface
		• **egress** --Captures traffic that is being transmitted by the interface.

Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. • Use this command only if you want to enable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 to enable NetFlow on other interfaces.	(Optional) --

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on Cisco Routers

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] cnfCINetflowEnable.*interface-number* **integer** [**0** | **1** | **2** | **3**]
2. Repeat Step 1 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] cnfCINetflowEnable.*interface-number* **integer** [**0**	**1**	**2**	**3**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1`	(Required) Configures NetFlow for an interface. • The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode. • The values for the *direction* argument are: ◦ 0--Disable NetFlow ◦ 1--Enable Ingress NetFlow ◦ 2--Enable Egress NetFlow ◦ 3--Enable Ingress and Egress NetFlow
Step 2	Repeat Step 1 to enable NetFlow on other interfaces	(Optional) --

Configuring NetFlow Top Talkers

This task describes the procedure for configuring the NetFlow Top Talkers feature. Perform the steps in this required task using either the router CLI commands or the SNMP commands to configure the NetFlow Top Talkers feature on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **top** *number*
5. **sort-by** [**bytes** | **packets**
6. **cache-timeout** *milliseconds*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	(Required) Enters NetFlow Top Talkers configuration mode.
Step 4	**top** *number* **Example:** `Router(config-flow-top-talkers)# top 50`	(Required) Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The range for the *number* argument is from 1 to 200 entries.
Step 5	**sort-by** [**bytes**	**packets** **Example:** `Router(config-flow-top-talkers)# sort-by packets`	(Required) Specifies the sort criterion for the top talkers. • The top talkers can be sorted either by the total number of packets of each top talker or the total number of bytes of each top talker.

	Command or Action	Purpose
Step 6	**cache-timeout** *milliseconds* **Example:** `Router(config-flow-top-talkers)# cache-timeout 30000`	(Optional) Specifies the amount of time that the list of top talkers is retained. • Reentering the **top**, **sort-by**, or **cache-timeout** command resets the timeout period, and the list of top talkers is recalculated the next time they are requested. • The list of top talkers is lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers. • If this timeout value is too large, the list of top talkers might not be updated quickly enough to display the latest top talkers. If a request to display the top talkers is made more than once during the timeout period, the same results will be displayed for each request. To ensure that the latest information is displayed while conserving CPU time, configure a large value for the timeout period and change the parameters of the **cache-timeout**, **top**, or **sort-by** command when a new list of top talkers is required. • The range for the *number* argument is from 1 to 3,600,000 milliseconds. The default is 5000 (5 seconds).
Step 7	**end** **Example:** `Router(config-flow-top-talkers)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow Top Talkers

SUMMARY STEPS

1. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTopN.0 unsigned** *number*
2. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsSortBy.0 integer** [**1** | **2** | **3**]
3. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsCacheTimeout.0 unsigned** *milliseconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTopN.0 unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsTopN.0 unsigned 50`	(Required) Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The value for the *number* argument in **cnfTopFlowsTopN.0** *number* is the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The range for the *number* argument is from 1 to 200 entries.
Step 2	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsSortBy.0 integer** [**1** | **2** | **3**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsSortBy.0 integer 2`	(Required) Specifies the sort criteria for the top talkers. • Values for *sort-option*in **cnfTopFlowsSortBy.0** [**1** | **2** | **3**] are ◦ 1--No sorting will be performed and that the NetFlow MIB and Top Talkers feature will be disabled. ◦ 2--Sorting will be performed by the total number of packets of each top talker. ◦ 3--Sorting will be performed by the total number of bytes of each top talker.
Step 3	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsCacheTimeout.0 unsigned** *milliseconds* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsCacheTimeout.0 unsigned 30000`	(Optional) Specifies the amount of time that the list of top talkers is retained. • Reentering the **top**, **sort-by**, or **cache-timeout** command resets the timeout period, and the list of top talkers is recalculated the next time they are requested. • The list of top talkers will be lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers. • If this timeout value is too large, the list of top talkers might not be updated quickly enough to display the latest top talkers. If a request to display the top talkers is made more than once during the timeout period, the same results will be displayed for each request. To ensure that the latest information is displayed while conserving CPU time, configure a large value for the timeout period and change the parameters of the **cache-timeout**, **top**, or **sort-by** command when a new list of top talkers is required. • The range for the *number* argument is from 1 to 3,600,000 milliseconds. The default is 5000 (5 seconds).

Configuring NetFlow Top Talkers Match Criteria

You can limit the traffic that is displayed by the NetFlow Top Talkers feature by configuring match criteria. The match criteria are applied to data in the main cache. The data in the main cache that meets the match criteria is displayed when you enter the **show ip flow top-talkers** command. To limit the traffic that is displayed by the NetFlow MIB and Top Talkers feature, perform the steps in this optional task.

Before configuring NetFlow MIB and Top Talkers match criteria, you should understand the following:

- NetFlow Top Talkers Match Criteria Specified by CLI Commands, page 157
- Configuring Source IP Address Top Talkers Match Criteria, page 159
- Configuring Source IP Address Top Talkers Match Criteria, page 160

NetFlow Top Talkers Match Criteria Specified by CLI Commands

You can use the **match** CLI command to specify match criteria to restrict the display of top talkers for the NetFlow MIB and Top Talkers feature. If you do not provide matching criteria, all top talkers are displayed.

Note When configuring a matching source, destination or nexthop address, both the address and a mask must be configured. The configuration will remain unchanged until both have been specified.

Note **cnfTopFlowsMatchSampler** matches flows from a named flow sampler. **cnfTopFlowsMatchClass** matches flows from a named class map.

Note When you are configuring the Top Talkers feature to match bytes and packets, the values that are matched are the total number of bytes and packets in the flow so far. For example, it is possible to match flows containing a specific number of packets, or flows with more or less than a set number of bytes.

For more information on using the match command, see the Cisco IOS NetFlow Command Reference.

- NetFlow Top Talkers Match Criteria Specified by SNMP Commands, page 157

NetFlow Top Talkers Match Criteria Specified by SNMP Commands

If you are using SNMP commands to configure NetFlow Top Talkers, see the table below for router CLI commands and equivalent SNMP commands.

Note Some of the SNMP match criteria options, such as the **cnfTopFlowsMatchSrcAddress** option, require that you enter more than one SNMP commands on the same line. For example, **snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal 172.16.10.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24**.

Table 31 Router CLI Commands and Equivalent SNMP Commands

Router CLI Command	SNMP Command
match source address [*ip-address*] [*mask* | */nn*]	**cnfTopFlowsMatchSrcAddress decimal** *ip-address* **cnfTopFlowsMatchSrcAddressType integer** *type* [4] **cnfTopFlowsMatchSrcAddressMask unsigned** *mask*
match destination address [*ip-address*][*mask* | */nn*]	**cnfTopFlowsMatchDstAddress decimal** *ip-address* **cnfTopFlowsMatchDstAddressType integer** *type1* **cnfTopFlowsMatchDstAddressMask unsigned** *mask*
match nexthop address [*ip-address*][*mask* | */nn*]	**cnfTopFlowsMatchNhAddress decimal** *ip-address* **cnfTopFlowsMatchNhAddressType integer** *type1* **cnfTopFlowsMatchNhAddressMask unsigned** *mask*
match source port min *port*	**cnfTopFlowsMatchSrcPortLo integer** *port*
match source port max *port*	**cnfTopFlowsMatchSrcPortHi integer** *port*
match destination port min *port*	**cnfTopFlowsMatchDstPortLo integer** *port*
match destination port max *port*	**cnfTopFlowsMatchDstPortHi integer** *port*
match source as *as-number*	**cnfTopFlowsMatchSrcAS integer** *as-number*
match destination as *as-number*	**cnfTopFlowsMatchDstAS integer** *as-number*
match input-interface *interface*	**cnfTopFlowsMatchInputIf integer** *interface*
match output-interface *interface*	**cnfTopFlowsMatchOutputIf integer** *interface*
match tos [*tos-value* | **dscp** *dscp-value* | **precedence** *precedence-value*]	**cnfTopFlowsMatchTOSByte integer** *tos-value* [5]
match protocol [*protocol-number* | **tcp** | **udp**]	**cnfTopFlowsMatchProtocol integer** *protocol-number*

4 The only IP version type that is currently supported is IPv4 (type 1).

5 tos-value is 6 bits for DSCP, 3 bits for precedence, and 8 bits (one byte) for ToS.

Router CLI Command	SNMP Command
match flow-sampler *flow-sampler-name*	**cnfTopFlowsMatchSampler string** *flow-sampler-name*
match class-map *class*	**cnfTopFlowsMatchClass string** *class*
match packet-range min *minimum-range*	**cnfTopFlowsMatchMinPackets unsigned** *minimum-range*
match packet-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets unsigned** *maximum-range*
match byte-range min *minimum-range*	**cnfTopFlowsMatchMinBytes unsigned** *minimum-range*
match byte-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets unsigned** *maximum-range*

Configuring Source IP Address Top Talkers Match Criteria

Perform the steps in this optional task using either the router CLI commands or the SNMP commands to add source IP address match criteria to the Top Talkers configuration.

For information on configuring other Top Talkers match criteria see the following resources:

- Cisco IOS NetFlow Command Reference.
- CISCO-NETFLOW-MIB at the following URL: http://www.cisco.com/go/mibs/ . Select SNMP Object Locator. Then select View & Download MIBs.

You must configure NetFlow Top Talkers before you perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **match source address** {*ip-address/nn* | *ip-address mask*}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	(Required) Enters NetFlow Top Talkers configuration mode.
Step 4	**match source address** {*ip-address/nn* | *ip-address mask*} **Example:** `Router(config-flow-top-talkers)# match source address 172.16.10.0 /24`	(Required) Specifies a match criterion. • The **source address** keyword specifies that the match criterion is based on the source IP address. • The *ip-address*argument is the IP address of the source, destination, or next-hop address to be matched. • The *mask* argument is the address mask, in dotted decimal format. • The */nn* argument is the address mask as entered in CIDR format. The **match source address** *172.16.10.0/24* is equivalent to the **match source address** *172.16.10.0 255.255.255.0* command. **Note** You must configure at least one of the possible match criteria before matching can be used to limit the traffic that is displayed by the NetFlow Top Talkers feature. Additional match criteria are optional. **Note** For a full list of the matching criteria that you can select, refer to NetFlow Top Talkers Match Criteria Specified by CLI Commands, page 157.
Step 5	**end** **Example:** `Router(config-flow-top-talkers)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Source IP Address Top Talkers Match Criteria

SUMMARY STEPS

1. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal 172.16.10.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24`	(Required) Specifies a match criterion. • The IP address type of 1 in the **cnfTopFlowsMatchSrcAddressType.0 integer 1** command specifies an IP version 4 (IPv4) address for the IP address type. IPv4 is currently the only IP version that is supported. • The *ip-address* argument in **cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* is the IPv4 source IP address to match in the traffic that is being analyzed. • The *mask* argument in **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask* is the number of bits in the mask for the IPv4 source IP address to match in the traffic that is being analyzed. **Note** You must configure at least one of the possible match criteria before matching can be used to limit the traffic that is displayed by the Top talkers feature. Additional match criteria are optional. **Note** To remove the **cnfTopFlowsMatchSrcAddress** match criterion from the configuration, specify an IP address type of 0 (unknown) with the cnfTopFlowsMatchSrcAddressType.0 integer 0 command. **Note** For a list of router CLI commands and their corresponding SNMP commands, see Configuring Source IP Address Top Talkers Match Criteria, page 160.

Verifying the NetFlow Top Talkers Configuration

To verify the NetFlow Top Talkers configuration, perform the steps in this optional task using either the router CLI command or the SNMP commands.

SUMMARY STEPS

1. **show ip flow top-talkers**

DETAILED STEPS

show ip flow top-talkers
Use this command to verify that the NetFlow MIB and Top Talkers feature is operational. For example:

Example:

```
Router# show ip flow top-talkers
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et3/0         10.1.1.3        Local         10.1.1.2        01 0000 0000  4800
Et3/0         10.1.1.4        Local         10.1.1.2        01 0000 0000  4800
```

```
Et3/0         10.1.1.5        Local         10.1.1.2        01 0000 0000   800
3 of 10 top talkers shown. 3 flows processed.
```

Verifying the NetFlow Top Talkers Configuration

In this example, even though a maximum of ten top talkers is configured by the **top** command, only three top talkers were transmitting data in the network. Therefore, three top talkers are shown, and the "3 flows processed" message is displayed in the output. If you expect more top talkers to be displayed than are being shown, this condition may possibly be the result of matching criteria, specified by the **match** command, that are overly restrictive.

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsGenerate.0 integer 1**
2. **snmpget -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsReportAvailable**
3. **snmpwalk -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTable**

DETAILED STEPS

Step 1 **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsGenerate.0 integer 1**
Use this command to initiate a generation of the top talkers statistics:

Example:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsGenerate.0 integer 1
CISCO-NETFLOW-MIB::cnfTopFlowsGenerate.0 = INTEGER: true(1)
```

Step 2 **snmpget -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsReportAvailable**
Use this command to verify that the top talkers statistics are available:

Example:

```
workstation% snmpwalk -c public -m all -v2c 10.4.9.62 cnfTopFlowsReportAvailable
CISCO-NETFLOW-MIB::cnfTopFlowsReportAvailable.0 = INTEGER: true(1)
```

Step 3 **snmpwalk -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTable**
Use this command to display the NetFlow top talkers:

Example:

```
workstation% snmpwalk -c public -m all -v2c 10.4.9.62 cnfTopFlowsTable
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddress.1 = Hex-STRING: 0A 04 09 08
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddressMask.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddress.1 = Hex-STRING: 0A 04 09 A7
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddressMask.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsNhAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsNhAddress.1 = Hex-STRING: 00 00 00 00
CISCO-NETFLOW-MIB::cnfTopFlowsSrcPort.1 = Gauge32: 32773
```

```
CISCO-NETFLOW-MIB::cnfTopFlowsDstPort.1 = Gauge32: 161
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsDstAS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsInputIfIndex.1 = INTEGER: 1
CISCO-NETFLOW-MIB::cnfTopFlowsOutputIfIndex.1 = INTEGER: 0
CISCO-NETFLOW-MIB::cnfTopFlowsFirstSwitched.1 = Timeticks: (12073160) 1 day, 9:32:11.60
CISCO-NETFLOW-MIB::cnfTopFlowsLastSwitched.1 = Timeticks: (12073160) 1 day, 9:32:11.60
CISCO-NETFLOW-MIB::cnfTopFlowsTOS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsProtocol.1 = Gauge32: 17
CISCO-NETFLOW-MIB::cnfTopFlowsTCPFlags.1 = Gauge32: 16
CISCO-NETFLOW-MIB::cnfTopFlowsSamplerID.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsClassID.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsFlags.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsBytes.1 = Gauge32: 75
CISCO-NETFLOW-MIB::cnfTopFlowsPackets.1 = Gauge32: 1
```

Tip You must convert the source and destination IP addresses from hexadecimal to dotted decimal format used in the display output before you can correlate them to source and destination hosts on your network. For example, in the display output above: 0A 04 09 02 = 10.4.9.2 and 0A 04 09 AF = 10.4.9.175.

Configuration Examples for NetFlow Top Talkers

- Configuring NetFlow Top Talkers Using SNMP Commands Example, page 163
- Configuring NetFlow Top Talkers Match Criteria Using SNMP Commands Example, page 164

Configuring NetFlow Top Talkers Using SNMP Commands Example

The following output from the network management workstation shows the command and the response for enabling NetFlow on interface GigabitEthernet6/2 (ifindex number 60):

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1
CISCO-NETFLOW-MIB::cnfCINetflowEnable.60 = INTEGER: interfaceDirIngress(1)
```

The following output from the network management workstation shows the command and the response for specifying 5 as the maximum number of top talkers that will be retrieved by a NetFlow top talkers query:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsTopN.0 unsigned 5
CISCO-NETFLOW-MIB::cnfTopFlowsTopN.0 = Gauge32: 5
```

The following output from the network management workstation shows the command and the response for specifying the sort criteria for the top talkers:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsSortBy.0 integer 2
CISCO-NETFLOW-MIB::cnfTopFlowsSortBy.0 = INTEGER: byPackets(2)
```

The following output from the network management workstation shows the command and the response for specifying the amount of time that the list of top talkers is retained:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsCacheTimeout.0 unsigned
2000
CISCO-NETFLOW-MIB::cnfTopFlowsCacheTimeout.0 = Gauge32: 2000 milliseconds
```

Configuring NetFlow Top Talkers Match Criteria Using SNMP Commands Example

The following output from the network management workstation shows the **snmpset** command and the response for specifying the following NetFlow Top Talkers match criteria:

- Source IP address-172.16.23.0
- Source IP address mask-255.255.255.0 (/24)
- IP address type-IPv4

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddress.0
decimal 172.16.23.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24
cnfTopFlowsMatchSrcAddressType.0 integer 1
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddress.0 = Hex-STRING: AC 10 17 00
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddressMask.0 = Gauge32: 24
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddressType.0 = INTEGER: ipv4(1)
```

The following output from the network management workstation shows the **snmpset** command and the response for specifying the class-map *my-class-map* as aNetFlow Top Talkers match criterion:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchClass.0 s my-class-
map
CISCO-NETFLOW-MIB::cnfTopFlowsMatchClass.0 = STRING: my-class-map.
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches

Related Topic	Document Title
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
CISCO-NETFLOW-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL (requires CCO login account): http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 32 Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands

Feature Name	Releases	Feature Configuration Information
NetFlow MIB	12.3(7)T, 12.2(25)S 12.2(27)SBC	The NetFlow MIB feature provides MIB objects to allow users to monitor NetFlow cache information, the current NetFlow configuration, and statistics. The following command was introduced by this feature: **ip flow-cache timeout**.

Feature Name	Releases	Feature Configuration Information
NetFlow MIB and Top Talkers	12.3(11)T, 12.2(25)S 12.2(27)SBC 12.2(33)SXH	The NetFlow MIB feature that was originally released in Cisco IOS Release12.3(7)T was modified in Cisco IOS Release 12.3(11)T to support the new NetFlow Top Talkers feature. The modifications to the NetFlow MIB and the new Top Talkers feature were released under the feature name NetFlow MIB and Top Talkers. The NetFlow MIB and Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications (top talkers) in the network. The NetFlow MIB component of the NetFlow MIB and Top Talkers feature enables you to configure top talkers and view the top talker statistics using SNMP. The following commands were introduced by this feature: **cache-timeout**, **ip flow-top-talkers**, **match**, **show ip flow top-talkers**, **sort-by**, and **top**.

Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

This document contains information about and instructions for configuring NetFlow Accounting for Unicast and Multicast on generic routing encapsulation (GRE) IP Tunnel Interfaces. NetFlow multicast accounting allows you to capture multicast-specific data (both packets and bytes) for multicast flows.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through a router. It is emerging as a primary network accounting and security technology.

- Finding Feature Information, page 169
- Prerequisites for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 170
- Restrictions for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 170
- Information About NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 170
- How to Configure NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces, page 175
- Configuration Examples for NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces, page 190
- Additional References, page 192
- Feature Information for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces, page 193

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

- You must use the Per-interface NetFlow feature in conjunction with the NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces feature.
- The instructions for configuring IPv4 unicast routing are not included in this document. If you want to configure NetFlow accounting for IPv4 unicast traffic on a GRE IP interface, your switch must already be configured for IPv4 unicast routing.
- The instructions for configuring IPv4 multicast routing are not included in this document. If you want to configure NetFlow accounting for IPv4 multicast traffic on a GRE IP interface, your switch must already be configured for IPv4 multicast routing.

Restrictions for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

- Only Catalyst 6500 series switches with a supervisor 720 is supported.
- Multicast flow packet and byte counters will be updated only in PFC3B mode and above.
- Only hardware switched flows are supported.
- Only Version 9 NetFlow data export format is supported.

Information About NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

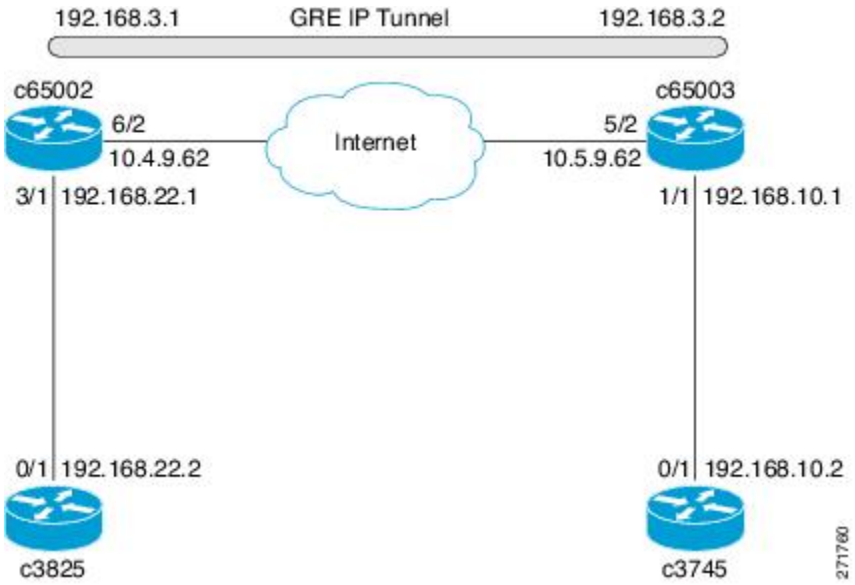
- GRE Tunneling, page 170
- GRE Tunnel Keepalive, page 171
- Tunnel Interfaces, page 171
- NetFlow Accounting on GRE IP Tunnel Interfaces, page 171

GRE Tunneling

Generic routing encapsulation (GRE) tunneling is defined in RFC 2784. GRE is a carrier protocol that can be used with a variety of underlying transport protocols and that can carry a variety of passenger protocols. RFC 2784 also covers the use of GRE with IPv4 as the transport protocol and the passenger protocol. For

more information on GRE tunnels, see the *Cisco IOS Interface and Hardware Component Configuration Guide* . The figure below is an example of a typical implementation of a GRE IP tunnel.

Figure 23 Sample Network with a GRE IPv4 Tunnel



GRE Tunnel Keepalive

Keepalive packets can be configured to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

Tunnel Interfaces

A tunnel interface is used to pass protocol traffic across a network that does not normally support the protocol. To build a tunnel requires defining a tunnel interface on each of two routers. The tunnel interfaces must reference each other. At each router, the tunnel interface must be configured with a Layer 3 address. The tunnel endpoints, tunnel source, and tunnel destination must be defined, and the type of tunnel must be selected. Optional steps can be performed to customize the tunnel.

Remember to configure the router at each end of the tunnel. If only one side of a tunnel is configured, the tunnel interface may still come up and stay up (unless keepalive is configured), but packets going into the tunnel will be dropped.

In Cisco IOS Release 12.2(8)T and later releases, Cisco express forwarding (CEF) switching over multipoint GRE tunnels was introduced. Previously, only process switching was available for multipoint GRE tunnels.

NetFlow Accounting on GRE IP Tunnel Interfaces

To analyze traffic that is sent from c3825 to c3745 in the figure below, NetFlow accounting is configured as shown in the table below. The flows in the "Flows" column are shown in the Unicast IPv4 Traffic over

an IPv4 Unicast GRE Tunnel (Encapsulation) figure through the Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation) figure.

Table 33 Where to Configure NetFlow Accounting and Which NetFlow Commands to Configure

Encapsulation/ De-encapsulation	Router	Ingress Physical Interface	Ingress Tunnel Interface	Egress Physical Interface	Egress Tunnel Interface	Flows
Traffic Direction						
Unicast over GRE (encap)	C650002 C3825 to C3745	**ip flow ingress** on interface gigabit 3/1	No configuration	No configuration	**ip flow egress** on interface tunnel 0	Flow (1) Flow (2)
Unicast over GRE (decap)	C65003 C3825 to C3745	**ip flow ingress** on interface gigabit 5/2	**ip flow ingress** on interface tunnel 0	No configuration	No configuration	Flow (1) Flow (2)
Multicast over GRE (encap)	C650002 C3825 to 3C745	**ip flow ingress** on interface gigabit 3/1	No configuration	**ip flow egress** on interface 6/2	**ip flow egress** on interface tunnel 0	Flow (1) Flow (2) Flow (3)
Multicast over GRE (decap)	C65003 C3825 to C3745	**ip flow ingress** on interface gigabit 5/2	**ip flow ingress** on interface tunnel 0	**ip flow egress** on interface 1/1	No configuration	Flow (1) Flow (2) Flow (3)

When you configure NetFlow accounting for IPv4 unicast traffic on a GRE tunnel interface, the traffic that is encapsulated or de-encapsulated on the router results in the creation of two flows. See the Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation) figure and the Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation) figure. When you configure NetFlow accounting for IPv4 multicast traffic on a GRE tunnel interface, the traffic that is encapsulated or de-encapsulated on the router results in the creation of three flows. See the Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation) figure and the Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation) figure. The increase in the number of flows created results in an increase in the usage of the hardware NetFlow table. You must monitor the hardware NetFlow table on your router to ensure that it is not oversubscribed.

If you are using NetFlow data export, the number of exported flows is also increased. Flows from the hardware table are converted to the Version 9 export format and then exported. Because the number of flows is doubled when you configure NetFlow Data Export, twice as much memory is required to convert the flows to Version 9 export format and then export them.

The table below provides the definitions of the terms used in the figures below.

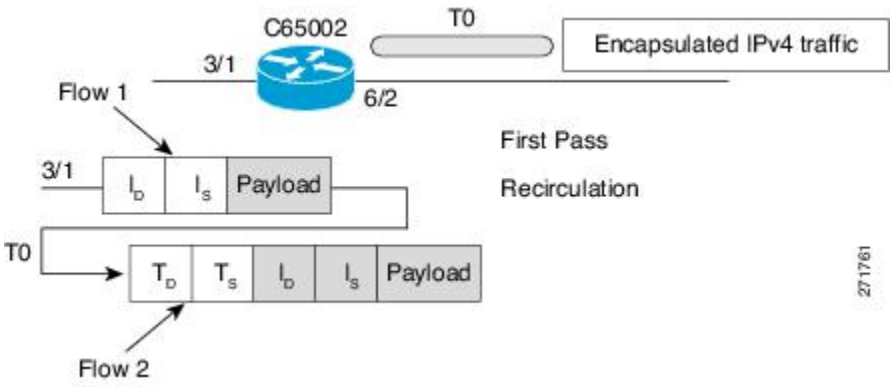
Table 34 Definition of Terms Used in Figures 2 through 5

Term	Definition
encapsulation	Adding the GRE tunnel header and trailer to the beginning and end respectively, of the packet being transmitted over the GRE tunnel.

Term	Definition
de-encapsulation	Removing the GRE tunnel header and trailer from the beginning and end respectively, of the packet being received from the GRE tunnel.
ingress	The inbound path of traffic. For example, the ingress interface is the interface over which traffic is received.
egress	The outbound path of traffic. For example, the egress interface is the interface over which traffic is transmitted.
ID	Destination IP address.
IS	Source IP address.
TD	Destination IP address for the tunnel interface.
TS	Source IP address for the tunnel interface.
MD	Multicast destination IP address.
MS	Multicast source IP address.
payload	The packet data.

The figure below shows the packet encapsulation process for unicast IPv4 traffic that is received on interface Gigabit Ethernet 3/1 on c65002 in the figure above. The first flow is the result of NetFlow accounting for the traffic after it is received on physical interface 3/1 (ingress NetFlow). The second flow is the result of NetFlow accounting for the traffic as it is being transmitted on the GRE tunnel interface T0 (egress NetFlow).

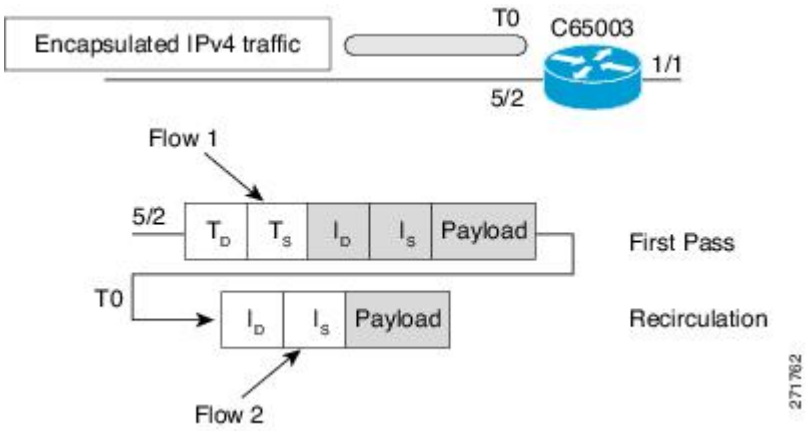
Figure 24 Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation)



The figure below shows the packet de-encapsulation process for unicast IPv4 traffic that is received on interface Gigabit Ethernet 3/1 on c65002 in the Sample Network with a GRE IPv4 Tunnel figure. The first flow is the result of NetFlow accounting for the traffic after it is received on the physical interface 5/2

(ingress NetFlow). The second flow is the result of NetFlow accounting for the traffic as it is being received and de-encapsulated on the tunnel interface T0 (ingress NetFlow).

Figure 25 Unicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation)

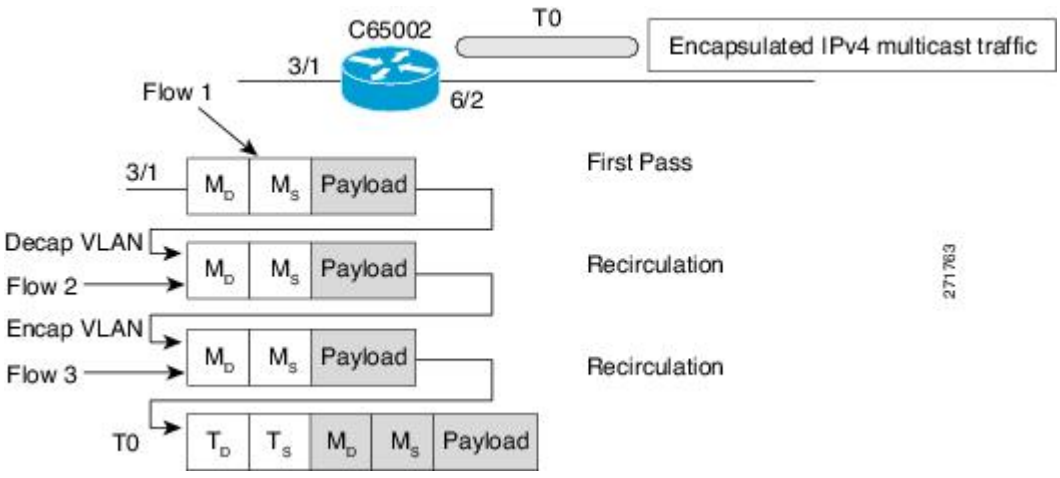


During de-encapsulation, only ingress features of the tunnel are applied on the packets, and during encapsulation, only egress features of the tunnel are applied.

Multicast replication can happen in either ingress or egress mode. GRE encapsulation of multicast flows is done on the line card on which the ingress physical interface resides, irrespective of the ingress or egress replication mode. So in the case of both ingress and egress multicast replication modes, egress flows are created on the ingress line card.

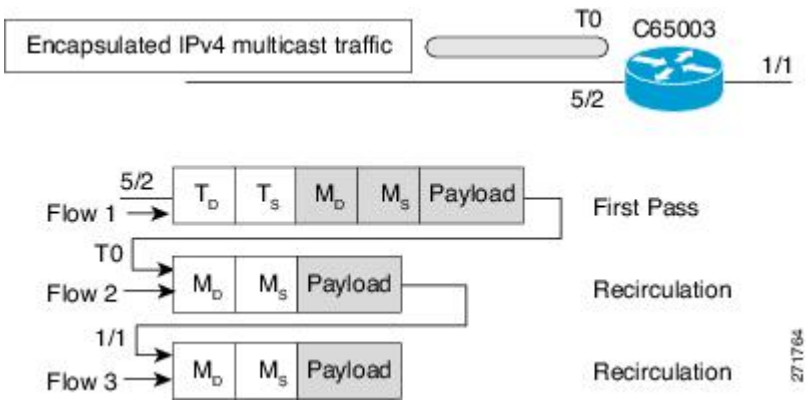
The examples in the figures below show how and why multiple flows are created during GRE handling of packets. In the figure below, Flow 1 is created when packets are received by physical interface 3/1. Flows 2 and 3 are created as part the multicast replication process using the internal virtual local area networks (VLANs) that are required for NetFlow accounting to keep track of the multicast traffic.

Figure 26 Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (Encapsulation)



In the figure below, Flow 1 is created when packets are received over physical interface 5/2. Flow 2 is created as part of the de-encapsulation process. Flow 3 is created as the multicast traffic is replicated and forwarded on interface 1/1.

Figure 27 Multicast IPv4 Traffic over an IPv4 Unicast GRE Tunnel (De-encapsulation)



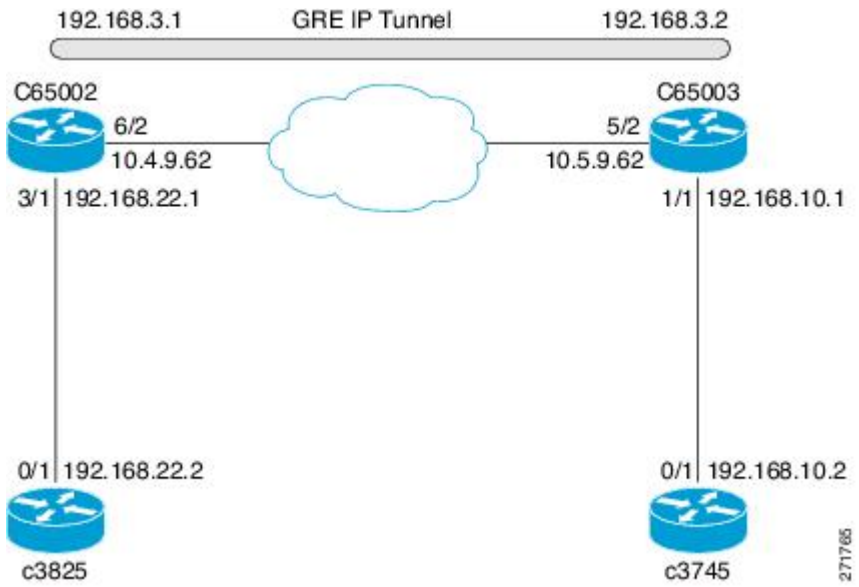
How to Configure NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces

- Sample Network, page 176
- Configuring a GRE IP Tunnel, page 176
- Verifying the Status of the GRE IP Tunnel, page 180
- Configuring NetFlow Accounting on a GRE IP Tunnel Interface, page 181
- Configuring NetFlow Accounting on the Physical Interfaces, page 182
- Verifying NetFlow Accounting, page 184
- Configuring NetFlow Data Export Using the Version 9 Export Format, page 186
- Verifying That NetFlow Data Export Is Operational, page 189

Sample Network

The tasks in this section use the sample network shown in the figure below.

Figure 28 Sample Network with a GRE IPv4 Tunnel



Configuring a GRE IP Tunnel

To configure a GRE IP tunnel as shown in Configuring a GRE IP Tunnel, page 176, perform the task in this section.

Ensure that the physical interface to be used as the tunnel source in this task is up and configured with the appropriate IP address. For hardware technical descriptions and information about installing interfaces, see the hardware installation and configuration documentation for your product.

Note GRE tunnel keepalive is not supported in cases where virtual route forwarding (VRF) is applied to a GRE tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bandwidth** *kbps*
5. **ip address** *address mask*
6. **keepalive** [*period* [*retries*]]
7. **tunnel source** {*ip-address* | *interface-type interface-number*}
8. **tunnel destination** {*hostname* | *ip-address*}
9. **tunnel key** *key-number*
10. **tunnel mode gre ip**
11. **ip mtu** *bytes*
12. **ip tcp mss** *mss-value*
13. **tunnel path-mtu-discovery** [**age-timer** {*aging-mins*| **infinite**}]
14. **end**
15. Repeat steps 1-14 on the router that hosts the other end of the GRE tunnel

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface tunnel 0`	Specifies the interface type and number and enters interface configuration mode. • To configure a tunnel, use *tunnel*for the *type* argument.

	Command or Action	Purpose
Step 4	**bandwidth** *kbps* **Example:** `Router(config-if)# bandwidth 1000`	Sets the current bandwidth value for an interface and communicates it to higher-level protocols. Specifies the tunnel bandwidth to be used to transmit packets. • Use the *kbps*argument to set the bandwidth, in kilobits per second (kbps). **Note** This is a routing parameter only; it does not affect the physical interface. The default bandwidth setting on a tunnel interface is 9.6 kbps. You should set the bandwidth on a tunnel to an appropriate value.
Step 5	**ip address** *address mask* **Example:** `Router(config-if)# ip address 192.168.3.1 255.255.255.0`	Specifies an IP address for the interface.
Step 6	**keepalive** [*period* [*retries*]] **Example:** `Router(config-if)# keepalive 3 7`	(Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down. • GRE keepalive packets may be configured either on only one side of the tunnel or on both. • If GRE keepalive is configured on both sides of the tunnel, the *period* and *retries* arguments can be different at each side of the link. **Note** This command is supported only on GRE point-to-point tunnels. **Note** The GRE tunnel keepalive feature should not be configured on a VRF tunnel. This combination of features is not supported.
Step 7	**tunnel source** {*ip-address* | *interface-type interface-number*} **Example:** `Router(config-if)# tunnel source GigabitEthernet6/2`	Configures the tunnel source. • Use the *ip-address*argument to specify the source IP address. • Use the *interface-type*and *interface-number*arguments to specify the interface to use. **Note** The tunnel source and destination IP addresses must be defined on two separate devices.
Step 8	**tunnel destination** {*hostname* | *ip-address*} **Example:** `Router(config-if)# tunnel destination 10.5.9.62`	Configures the tunnel destination. • Use the *hostname*argument to specify the name of the host destination. • Use the *ip-address*argument to specify the IP address of the host destination. **Note** The tunnel source and destination IP addresses must be defined on two separate devices.

	Command or Action	Purpose
Step 9	**tunnel key** *key-number* **Example:** `Router(config-if)# tunnel key 1000`	(Optional) Enables an ID key for a tunnel interface. • Use the *key-number*argument to identify a tunnel key that is carried in each packet. • Tunnel ID keys can be used as a form of weak security to prevent improper configuration or injection of packets from a foreign source. **Note** This command is supported only on GRE tunnel interfaces. We do not recommend relying on this key for security purposes.
Step 10	**tunnel mode gre ip** **Example:** `Router(config-if)# tunnel mode gre ip`	Specifies **GRE IP** as the encapsulation protocol to be used in the tunnel.
Step 11	**ip mtu** *bytes* **Example:** `Router(config-if)# ip mtu 1400`	(Optional) Set the maximum transmission unit (MTU) size of IP packets sent on an interface. • If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it unless the don't fragment (DF) bit is set. • All devices on a physical medium must have the same protocol MTU in order to operate. **Note** If the **tunnel path-mtu-discovery** command is going to be enabled in Configuring a GRE IP Tunnel, page 176, do not configure this command.
Step 12	**ip tcp mss** *mss-value* **Example:** `Router(config-if)# ip tcp mss 250`	(Optional) Specifies the maximum segment size (MSS) for TCP connections that originate or terminate on a router. • Use the *mss-value* argument to specify the maximum segment size for TCP connections, in bytes.
Step 13	**tunnel path-mtu-discovery** [**age-timer** {*aging-mins*| **infinite**}] **Example:** `Router(config-if)# tunnel path-mtu-discovery`	(Optional) Enables Path MTU Discovery (PMTUD) on a GRE or IP-in-IP tunnel interface. • When PMTUD is enabled on a tunnel interface, PMTUD will operate for GRE IP tunnel packets to minimize fragmentation in the path between the tunnel endpoints.
Step 14	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 15	Repeat steps 1-14 on the router that hosts the other end of the GRE tunnel	--

Verifying the Status of the GRE IP Tunnel

To verify the tunnel configuration and operation, perform the following optional task:

SUMMARY STEPS

1. **enable**
2. **ping** *ip-address*
3. **ping** *ip-address*
4. **show interfaces tunnel** *number* [**accounting**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **ping** *ip-address*
To verify that each router has IP connectivity to the tunnel endpoint on the other router, ping the IP address of the remote tunnel endpoint from the local router.

Example:

```
c65002# ping
 192.168.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

Step 3 **ping** *ip-address*
To verify that each router has IP connectivity to the tunnel endpoint on the other router, ping the IP address of the remote tunnel endpoint from the local router.

Example:

```
c65003# ping
 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
```

Step 4 **show interfaces tunnel** *number* [**accounting**
Displays the status and statistics of the tunnel interface

Example:

```
c65002# show interface tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.3.1/24
  MTU 1514 bytes, BW 1000 Kbit, DLY 50000 usec,
     reliability 255/255, txload 115/255, rxload 57/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.4.9.62 (GigabitEthernet6/2), destination 10.5.9.62
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Path MTU Discovery, ager 10 mins, min MTU 92
  Last input 00:07:35, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 4139000 bits/sec, 659 packets/sec
  5 minute output rate 4117000 bits/sec, 669 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     245049 packets input, 192533770 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     251500 packets output, 196216398 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuring NetFlow Accounting on a GRE IP Tunnel Interface

To configure NetFlow on a GRE IP tunnel interface, perform the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast netflow output-counters**
4. **interface tunnel** *number*
5. **ip flow** {**ingress** | **egress**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast netflow output-counters** **Example:** `Router(config)# ip multicast netflow output-counters`	(Optional) Enables NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow.
Step 4	**interface tunnel** *number* **Example:** `Router(conf)# interface tunnel 0`	Specifies the tunnel interface and enters interface configuration mode.
Step 5	**ip flow** {**ingress** | **egress**} **Example:** `Router(conf-if)# ip flow egress`	Configures NetFlow accounting on the interface. • **ingress** --Configures NetFlow accounting for traffic that is received by the interface. • **egress** --Configures NetFlow accounting for traffic that is transmitted by the interface.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring NetFlow Accounting on the Physical Interfaces

To configure NetFlow accounting on one or more physical interfaces, perform the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast netflow output-counters**
4. **interface** *type number*
5. Do one of the following:
   - **ip flow** {**ingress** | **egress**}
6. **exit**
7. Repeat Steps 4 through 6 to enable NetFlow on other interfaces.
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast netflow output-counters** **Example:** `Router(config)# ip multicast netflow output-counters`	(Optional) Enables NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 3/1`	Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.

	Command or Action	Purpose

Step 5	Do one of the following:
	• **ip flow** {**ingress** | **egress**}
	Example:
	`Router(config-if)# ip flow ingress`
	Example:
	Example:
	`Router(config-if)# ip flow egress`
		Enables NetFlow on the interface.
		• **ingress** --Captures traffic that is being received by the interface.
		• **egress** --Captures traffic that is being transmitted by the interface.

Step 6	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You need to use this command only if you want to enable NetFlow on another interface.
Step 7	Repeat Steps 4 through 6 to enable NetFlow on other interfaces.	(Optional) --
Step 8	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying NetFlow Accounting

To verify that NetFlow accounting for the tunnel interface is working, perform the following task.

Note This task uses the sample network shown in the figure below.

SUMMARY STEPS

1. **enable**
2. **show ip cache flow**
3. **show mls net ip module** *number*

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show ip cache flow**

The **show ip cache flow** command displays the NetFlow statistics in the cache. The tunnel interface (Tu0) appears in several rows of the statistics, indicating that NetFlow accounting is operational for the tunnel interface.

Example:

```
c65003# show ip cache flow
------------------------------------------------------------------------------
Displaying software-switched flow entries on the MSFC in Module 5:
IP packet size distribution (3721891 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 6 added
  5394 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 05:58:56
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 4      0.0    406293  1499     75.4     626.5      12.3
Total:               4      0.0    406293  1499     75.4     626.5      12.3
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa3/1         192.168.22.2    Tu0*          192.168.10.2    01 0000 0000  1052K
Fa3/1         192.168.22.2    Tu0           192.168.10.2    01 0000 0000  1052K
------------------------------------------------------------------------------
Displaying hardware-switched flow entries in the PFC (Active) Module 5:
 SrcIf            SrcIPaddress     DstIf            DstIPaddress    Pr SrcP DstP  Pkts
 Tu0              10.4.9.62        Gi6/2            10.5.9.62       2F 0000 0000   155K
 --               0.0.0.0          ---              0.0.0.0         00 0000 0000  1764K
 Fa3/1            192.168.22.2     Tu0              192.168.10.2    01 0000 0000    65K
 Tu0              192.168.10.2     Fa3/1            192.168.22.2    01 0000 0000   695K
 Tu0              192.168.10.2     Fa3/1            192.168.22.2    01 0008 0000    66K
 Tu0              192.168.10.2     Fa3/1            192.168.22.2    11 F378 F566    90K
 Fa3/1            192.168.22.2     Tu0              192.168.10.2    11 F566 F378    90K
```

Step 3 **show mls net ip module** *number*

The **show mls net ip mod** *number* command displays information about the hardware-switched NetFlow flows. The tunnel interface (Tu0) appears in several rows of the statistics, indicating that NetFlow accounting is operational for the tunnel interface.

Example:

```
c65003# show mls net ip module 5
Displaying NetFlow entries in Active Supervisor EARL in module 5
```

```
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f          :AdjPtr
--------------------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
------------------------------------------------
224.0.0.2       10.4.9.254      udp :646    :646      Gi6/2            :0x0
46           2852          200   00:30:28   Multicast
0.0.0.0         0.0.0.0         0   :0      :0        --               :0x0
238          17450         203   00:30:28   L3 - Dynamic
224.0.0.13      172.31.0.2      103 :0      :0        Gi6/2            :0x0
7            378           189   00:30:21   Multicast
224.0.0.5       192.168.255.254 89  :0      :0        Fa3/1            :0x0
204          16320         204   00:30:31   Multicast
224.0.0.1       172.31.0.2      2   :0      :0        Gi6/2            :0x0
3            138           174   00:29:38   Multicast
10.4.9.255      10.4.9.2        udp :138    :138      Fa3/1            :0x0
0            0             143   00:28:09   L3 - Dynamic
224.0.0.13      192.168.3.2     103 :0      :0        Tu0              :0x0
6            372           153   00:30:28   Multicast
224.192.16.1    172.31.0.1      icmp:0      :0        Fa3/1            :0x0
20435        940010        205   00:30:32   Multicast
224.0.0.1       192.168.3.2     2   :0      :0        Tu0              :0x0
2            64            103   00:29:49   Multicast
10.4.9.255      10.4.9.2        udp :137    :137      Fa3/1            :0x0
0            0             79    00:30:10   L3 - Dynamic
```

Configuring NetFlow Data Export Using the Version 9 Export Format

To configure NetFlow Data Export using the Version 9 data export format, perform the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls flow ip** {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}
4. **mls nde sender**
5. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*
6. Repeat Step 5 once to configure a second NetFlow export destination.
7. **ip flow-export source** *interface-type interface-number*
8. **ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]**
9. **ip flow-export template refresh-rate** *packets*
10. **ip flow-export template timeout-rate** *minutes*
11. **ip flow-export template options export-stats**
12. **ip flow-export template options refresh-rate** *packets*
13. **ip flow-export template options timeout-rate** *minutes*
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mls flow ip** {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**} **Example:** `Router(conf)# mls flow ip interface-full`	Specifies the flow mask for NetFlow data export.
Step 4	**mls nde sender** **Example:** `Router(config)# mls nde sender`	Enables multi-layer switching (MLS) NetFlow data export (NDE).
Step 5	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	Specifies the IP address or hostname of the NetFlow collector and the UDP port on which the NetFlow collector is listening.
Step 6	Repeat Step 5 once to configure a second NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.
Step 7	**ip flow-export source** *interface-type interface-number* **Example:** `Router(config)# ip flow-export source gigabitethernet 6/2`	(Optional) Specifies the interface from which the source IP address is derived for the UDP datagrams that are sent by NetFlow data export to the destination host.

	Command or Action	Purpose
Step 8	**ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]** **Example:** `Router(config)# ip flow-export version 9`	(Optional) Enables the export of information in NetFlow cache entries. • The **version 9** keyword specifies that the export packet uses the Version 9 format. • The **origin-as** keyword specifies that export statistics include the originating autonomous system for the source and destination. • The **peer-as** keyword specifies that export statistics include the peer autonomous system for the source and destination. • The **bgp-nexthop** keyword specifies that export statistics include border gateway protocol (BGP) next hop-related information. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card CEF tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 9	**ip flow-export template refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template refresh-rate 15` **Example:**	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are resent. Range is 1 to 600 packets. The default is 20 packets.
Step 10	**ip flow-export template timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template timeout-rate 90`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies that the **timeout-rate** keyword applies to the template. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are resent. You can specify from 1 to 3600 minutes. The default is 30 minutes.
Step 11	**ip flow-export template options export-stats** **Example:** `Router(config)# ip flow-export template options export-stats`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **export-stats**keyword specifies that the export statistics include the total number of flows exported and the total number of packets exported.

	Command or Action	Purpose
Step 12	**ip flow-export template options refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template options refresh-rate 25`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are resent. Range is 1 to 600 packets. The default is 20 packets.
Step 13	**ip flow-export template options timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template options timeout-rate 120`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are resent. Range is 1 to 3600 minutes. The default is 30 minutes.
Step 14	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying That NetFlow Data Export Is Operational

To verify that NetFlow data export is operational, perform the following optional task.

SUMMARY STEPS

1. **show ip flow export**
2. **show ip flow export template**

DETAILED STEPS

Step 1 **show ip flow export**

Use this command to display the statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

Example:

```
Router# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       10.4.9.62 (GigabitEthernet6/2)
    Source(2)       10.4.9.62 (GigabitEthernet6/2)
    Destination(1)  172.16.10.2 (99)
    Destination(2)  172.16.10.3 (99)
  Version 9 flow records
```

```
  11 flows exported in 11 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
  0 export packets were dropped due to Card not being able to export
```

Step 2 **show ip flow export template**

Use this command to display the statistics for the NetFlow data export (such as the template timeout rate and the refresh rate) for the template-specific configurations. The following is sample output from this command:

Example:

```
Router# show ip flow export template
Template Options Flag = 1
   Total number of Templates added = 1
   Total active Templates = 1
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 1
   Option  Templates added = 1
   Template ager polls = 0
   Option Template ager polls = 388
Main cache version 9 export is enabled
 Template export information
   Template timeout = 90
   Template refresh rate = 15
 Option export information
   Option timeout = 120
   Option refresh rate = 25
```

Configuration Examples for NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces

- Configuring a GRE IP Tunnel Example, page 190
- Configuring NetFlow Accounting on a GRE IP Tunnel Example, page 191

Configuring a GRE IP Tunnel Example

The following example shows how to configure a GRE IP tunnel:

```
interface Tunnel0
 tunnel mode gre ip
 bandwidth 1000
 ip address 192.168.3.1 255.255.255.0
 tunnel source GigabitEthernet6/2
 tunnel destination 10.5.9.62
 tunnel path-mtu-discovery
```

The following display output shows that the GRE IP tunnel is operational because the tunnel is transmitting and receiving traffic:

```
c65002# show interface tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.3.1/24
  MTU 1514 bytes, BW 1000 Kbit, DLY 50000 usec,
     reliability 255/255, txload 90/255, rxload 98/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.4.9.62 (GigabitEthernet6/2), destination 10.5.9.62
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Path MTU Discovery, ager 10 mins, min MTU 92
  Last input 00:11:44, output 00:11:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 380000 bits/sec, 125 packets/sec
  5 minute output rate 347000 bits/sec, 125 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     3344121 packets input, 2452613051 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     3399211 packets output, 2431569783 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuring NetFlow Accounting on a GRE IP Tunnel Example

The following example shows how to configure NetFlow Accounting on a GRE IP Tunnel and a FastEthernet interface:

```
mls flow ip interface-full
interface tunnel 0
 ip flow egress
 ip flow ingress
interface FastEthernet3/1
 no shut
 ip address 192.168.22.1 255.255.255.0
 ip flow ingress
 ip flow egress
```

The following display output shows that NetFlow accounting is operational because the flow cache has NetFlow statistics data in it:

```
c65002# show ip cache flow
------------------------------------------------------------------------------
Displaying software-switched flow entries on the MSFC in Module 5:
IP packet size distribution (3721891 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 6 added
  5394 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
```

```
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 05:58:56
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 4      0.0    406293  1499     75.4     626.5      12.3
Total:               4      0.0    406293  1499     75.4     626.5      12.3
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa3/1         192.168.22.2    Tu0*          192.168.10.2    01 0000 0000  1052K
Fa3/1         192.168.22.2    Tu0           192.168.10.2    01 0000 0000  1052K
------------------------------------------------------------------------------
Displaying hardware-switched flow entries in the PFC (Active) Module 5:
 SrcIf            SrcIPaddress     DstIf            DstIPaddress    Pr SrcP DstP  Pkts
 Tu0              10.4.9.62        Gi6/2            10.5.9.62       2F 0000 0000   155K
 --               0.0.0.0          ---              0.0.0.0         00 0000 0000  1764K
 Fa3/1            192.168.22.2     Tu0              192.168.10.2    01 0000 0000    65K
 Tu0              192.168.10.2     Fa3/1            192.168.22.2    01 0000 0000   695K
 Tu0              192.168.10.2     Fa3/1            192.168.22.2    01 0008 0000    66K
 Tu0              192.168.10.2     Fa3/1            192.168.22.2    11 F378 F566    90K
 Fa3/1            192.168.22.2     Tu0              192.168.10.2    11 F566 F378    90K
```

The following display output shows that NetFlow accounting is operational because there are statistics for the hardware-switched NetFlow flows.

```
c65003# show mls net ip mod 5
Displaying NetFlow entries in Active Supervisor EARL in module 5
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f          :AdjPtr
------------------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
-----------------------------------------------
224.0.0.2       10.4.9.254      udp :646    :646      Gi6/2            :0x0
46           2852          200   00:30:28   Multicast
0.0.0.0         0.0.0.0         0   :0      :0        --               :0x0
238          17450         203   00:30:28   L3 - Dynamic
224.0.0.13      172.31.0.2      103 :0      :0        Gi6/2            :0x0
7            378           189   00:30:21   Multicast
224.0.0.5       192.168.255.254 89  :0      :0        Fa3/1            :0x0
204          16320         204   00:30:31   Multicast
224.0.0.1       172.31.0.2      2   :0      :0        Gi6/2            :0x0
3            138           174   00:29:38   Multicast
10.4.9.255      10.4.9.2        udp :138    :138      Fa3/1            :0x0
0            0             143   00:28:09   L3 - Dynamic
224.0.0.13      192.168.3.2     103 :0      :0        Tu0              :0x0
6            372           153   00:30:28   Multicast
224.192.16.1    172.31.0.1      icmp:0      :0        Fa3/1            :0x0
20435        940010        205   00:30:32   Multicast
224.0.0.1       192.168.3.2     2   :0      :0        Tu0              :0x0
2            64            103   00:29:49   Multicast
10.4.9.255      10.4.9.2        udp :137    :137      Fa3/1            :0x0
0            0             79    00:30:10   L3 - Dynamic
```

Additional References

Related Documents

Related Topic	Document Title
Configuring Cisco IOS 12.2SX on Cisco Catalyst 6500 series switches	Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide

Standards

Standard	Title
There are no standards associated with this feature.	--

MIBs

MIB	MIBs Link
There are no MIBs associated with this feature.	--

RFCs

RFC	Title
RFC 2784	Generic Routing Encapsulation (GRE)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Accounting for Unicast and Multicast on GRE IP Tunnel Interfaces

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 35 Feature Information for Flexible NetFlow

Feature Name	Releases	Feature Configuration Information
Configuring NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces	12.2(33)SXI	The Configuring NetFlow Accounting for Unicast and Multicast on GRE Tunnel Interfaces feature allows NetFlow statistics to be gathered on traffic that is transmitted over a GRE IP tunnel interface. The following section provides information for configuring this feature: No commands were introduced or modified for this feature.